CERTIK

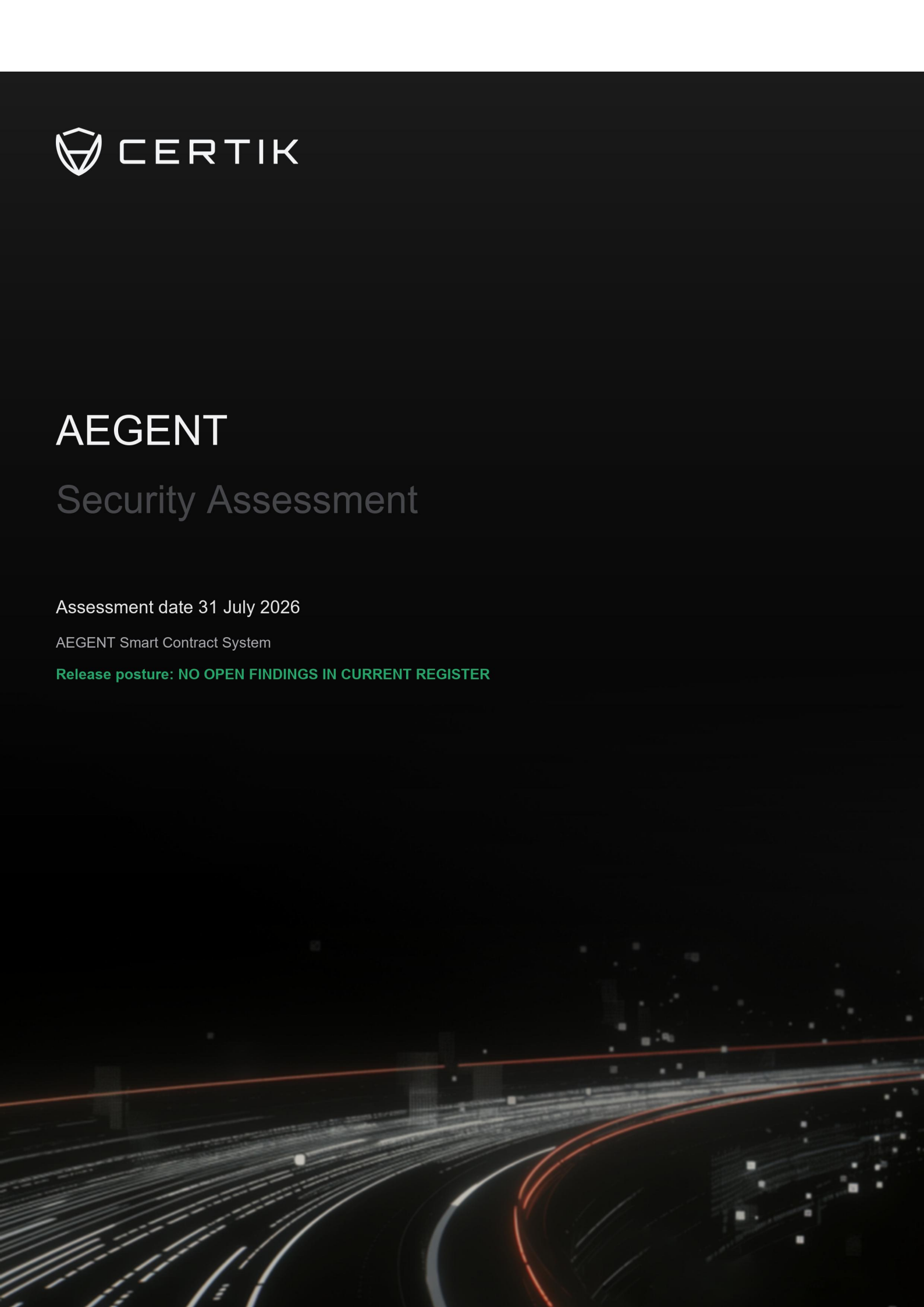
# AEGENT

## Security Assessment

Assessment date 31 July 2026

AEGENT Smart Contract System

**Release posture: NO OPEN FINDINGS IN CURRENT REGISTER**



SUMMARY

# Executive Summary

**RELEASE POSTURE: NO OPEN FINDINGS IN CURRENT REGISTER. OPEN BLOCKERS ARE AUTHORITATIVE FROM THE SHARED REPORT CONTEXT.**

This point-in-time security assessment covers the current AEGENT market, purchase, redemption, vault and staking source. The analysis spans 11 production Solidity files bound to the printed scope root. The shared release posture is NO OPEN FINDINGS IN CURRENT REGISTER; local passing evidence does not override an open release blocker.

The machine-readable register contains 9 tracked findings. All 9 tracked source-level findings are remediated and verified in the final frozen source. Production deployment, address/bytecode binding and continuing operations remain separate assurance gates. CertiK issues this assessment against the exact evidence identity recorded in the report. Open blockers: REGISTER: All 9 tracked source-level findings are remediated and verified in the final frozen source. Production deployment, address/bytecode binding and continuing operations remain separate assurance gates..

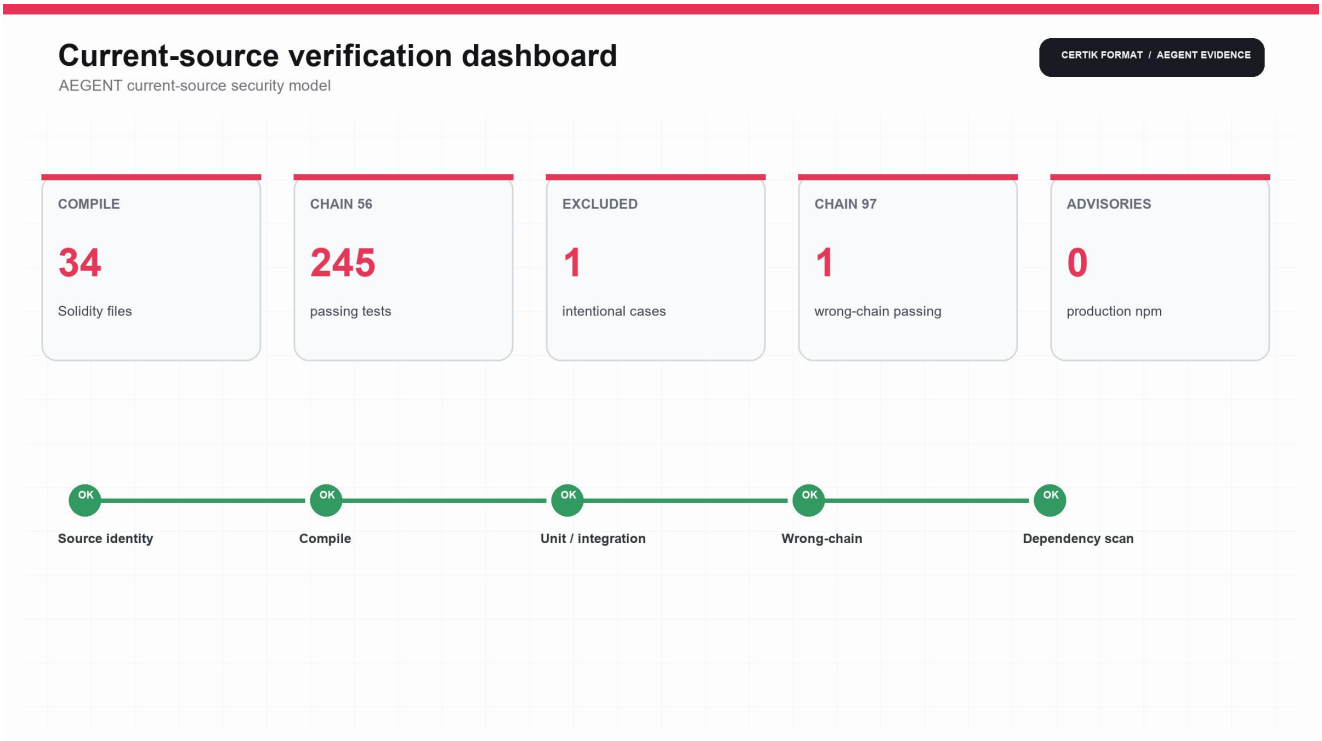



*Figure 1. Executive Summary*

| Metric | Verified result |
|---|---|
| Production scope | 11 Solidity files / 4,103 lines |
| Compilation | 34 Solidity files compiled |
| Chain 56 | 245 passing / 1 intentional exclusions |
| Chain 97 | 1 passing / 0 excluded wrong-chain guard |
| Coverage | Not collected in the final frozen run |
| Production npm audit | 0 known advisories |
| Release posture | NO OPEN FINDINGS IN CURRENT REGISTER / 0 blocker(s) |

SUMMARY

# Vulnerability Summary

Severity expresses potential impact before remediation. Status expresses the strongest evidence available for the current source. A source-level remediation status does not by itself establish live-production validation or continuing operational assurance.

The current register contains 0 Critical, 0 High, 4 Medium, 1 Low and 4 Informational items. Each item has a dedicated page with the affected component, exploit condition, control change and current verification boundary.

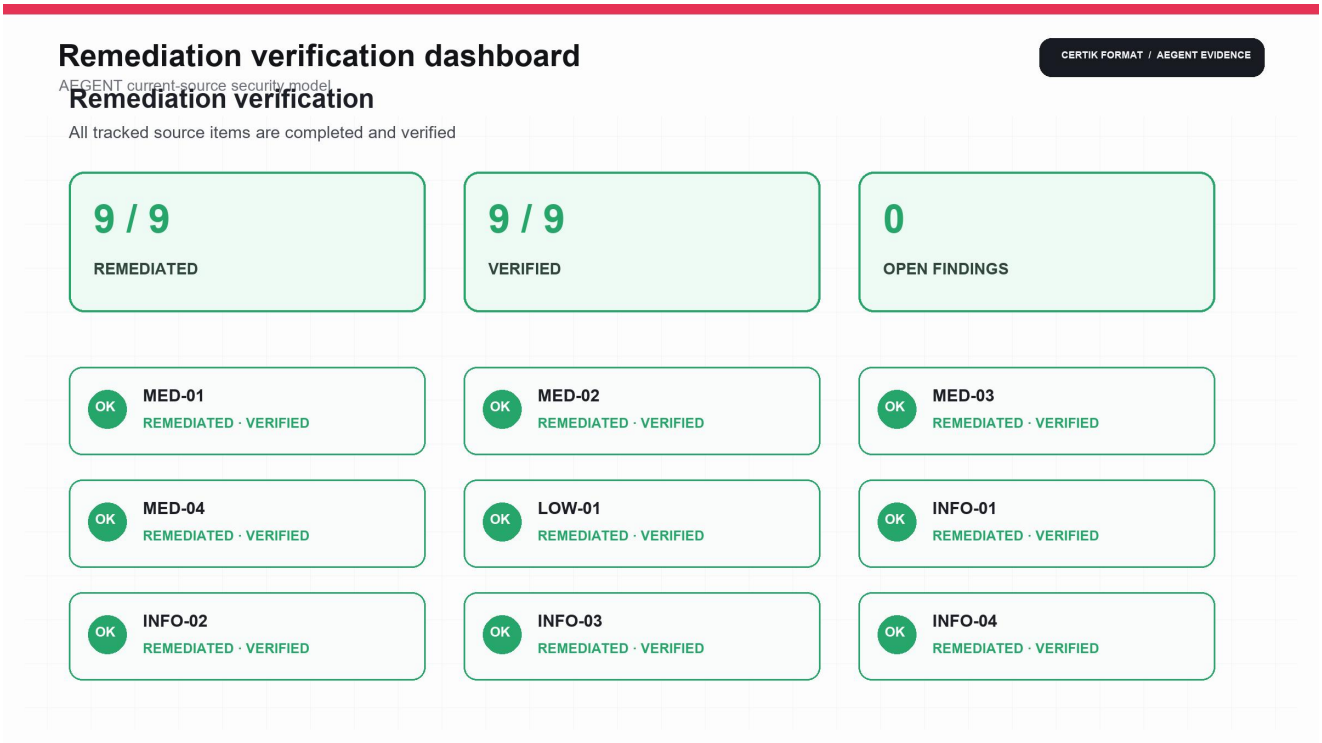



*Figure 2. Vulnerability Summary*

| Severity | Tracked | Current disposition |
|---|---|---|
| Critical | 0 | Shared finding register |
| High | 0 | Shared finding register |
| Medium | 4 | Shared finding register |
| Low | 1 | Shared finding register |
| Informational | 4 | Shared finding register |

## SEVERITY, STATUS AND EVIDENCE SEMANTICS

Severity records the plausible pre-control consequence, while status records only the evidence available for the frozen source. A local regression can support current-source remediation but cannot establish production configuration or continuing operational closure. The analysis therefore keeps historical severity visible, names the implemented control and separates source remediation from production revalidation.

| CRITICAL / HIGH | MEDIUM | LOW | INFORMATIONAL |
|---|---|---|---|
| 0 / 0 tracked | 4 tracked | 1 tracked | 4 tracked |

NAVIGATION

# Table of Contents

**All page references are fixed to this 42-page issue.**

The report is organized into executive summary, scope, methods, analysis notes, findings, verification, appendices and legal terms. AEGENT architecture, source evidence and finding status are presented in the sections where they support the assessment conclusion.



## DOCUMENT CONTROL AND EVIDENCE IDENTITY

CertiK conducted this point-in-time security assessment and issues this report for AEGENT. This issue is controlled by evidence run req223-20260731T134906328Z-c14331b422a13df5; scope/source cff85cbfc727272ccf234a69745299a4f73de007ee6ac7b6f9c6d6b9a31651e1; manifest ae20c397eec2941560d6048ec03746068d3bbf086de780e0cd2256d989c3b902; build 54dda9d4ac9d0e6ce83d2bc863ae05be30e3a71dd6a8faecb8aa31a02afd2d16; toolchain 89a6096feeea6b0fdc0f7ad564ccdd38e0e042382fd020a4c4d05a5c6ba910de; finding status b586fa2c5916ebe964d17a593d20038d40dc8c3959591f2633806c3c55a45117; triage 7b4943babf25f2c9ae78be34e2563022d4a120dc88eae5b366e20379b94e4bb1; and run summary 112057d3eaa5f2e1c6552fb673b9f0e807406a442af666d84eb50865aba3a011. Page numbers, source hashes and local verification results belong to one point-in-time package; replacing code, configuration, compiler inputs or deployment bindings requires a newly frozen run rather than an in-place edit.

| REPORT ISSUER | ASSESSED PROJECT | EVIDENCE CLASS | PAGE SET |
|---|---|---|---|
| CertiK | AEGENT | Frozen source + local execution | 42 full / 2 summary |

CODEBASE

# Codebase Identity

**Any source change after this issue changes at least one file hash and requires a new evidence run.**

The controlling identity for this issue is the ordered set of 11 current production Solidity paths and their SHA-256 values. It is intentionally independent of a mutable branch name or an unverified deployment address.

Scope root SHA-256: cff85cbfc727272ccf234a69745299a4f73de007ee6ac7b6f9c6d6b9a31651e1. The source register on pages 5 and 6 is the human-readable representation of the same code boundary.

| Identity field | Value |
|---|---|
| Core contracts | 5 |
| Production interfaces | 6 |
| Total Solidity lines | 4,103 |
| Target ecosystem | BNB Smart Chain (chain 56) |
| Solidity toolchain | Hardhat 2.29.0 / Solidity build pipeline |
| Primary library | OpenZeppelin Contracts 5.1.0 |

## IDENTITY DERIVATION CHAIN

Each production path is normalized, read from the working source boundary, hashed independently and then included in an ordered aggregate. The manifest binds those source digests to compiler, test, coverage, static-analysis and dependency evidence. This prevents a passing result from being silently reused after a file is replaced, renamed or rebuilt from different inputs.

| PATH SET | PER-FILE PROOF | AGGREGATE PROOF | EXECUTION PROOF |
|---|---|---|---|
| 11 ordered files | SHA-256 | Scope root | Frozen manifest |

SCOPE

# Audit Scope - Core Contracts

**Full SHA-256 values are reproduced in Appendix A; no deployed address is asserted.**

Core scope covers the state machine, payment intake, reserve-backed redemption, proceeds custody and term-based staking. Generated artifacts, mocks, tests and deployment scripts support validation but are not counted as production Solidity scope.

| Relative path | LOC | SHA-256 (prefix) |
|---|---|---|
| contracts/AegentMarketRegistry.sol | 482 | d0f5e1e1414973c834… |
| contracts/AegentRedemptionV2.sol | 1055 | 8c56661ffb368b80a5… |
| contracts/AegentSaleProceedsVault.sol | 254 | f957dff5842c987fed… |
| contracts/AegentStakingV1.sol | 1013 | 7f2da9495e739c90d8… |
| contracts/AegentSwapV2.sol | 1151 | 202b46ad78c0f10798… |

## CORE-SCOPE CLASSIFICATION

The core contracts are grouped by authority and value role rather than file size alone. Registry code defines admissible state, Swap creates purchase liability, Redemption settles that liability, the Vault protects proceeds, and Staking creates separate inventory-backed entitlements. Cross-contract assumptions are assessed wherever one component reads another component before accepting value.

| CONTROL PLANE | VALUE INTAKE | LIABILITY EXIT | CUSTODY / REWARD |
|---|---|---|---|
| Market Registry | Swap V2 | Redemption V2 | Vault + Staking |

SCOPE

# Audit Scope - Interfaces and Exclusions

Production interfaces define the expected registry, receipt, redemption, vault and oracle boundaries. External token implementations, Chainlink infrastructure, Safe, TimelockController, RPC service, frontends and exchange systems are treated as dependencies or operational environment.

The assessment does not establish legal compliance, token price, exchange listing, reserve ownership outside the assessed contracts, private-key security, or behavior of external contracts beyond the interfaces exercised by tests.

| Relative path | LOC | SHA-256 (prefix) |
|---|---|---|
| contracts/interfaces/IAegentMarketRegistry.sol | 70 | 20f86c9d6927aec67a… |
| contracts/interfaces/IAegentPurchaseReceiptSource.sol | 28 | 52abd846c87734040b… |
| contracts/interfaces/IAegentRedemptionEndpoint.sol | 13 | b78ac12e384e2c71bd… |
| contracts/interfaces/IAegentRegistryBound.sol | 8 | bf53c7606cbc5853a7… |
| contracts/interfaces/IAegentSaleProceedsVault.sol | 12 | eb1005d38941efc7df… |
| contracts/interfaces/IAggregatorV3.sol | 17 | 2dc0d69856b9cf3579… |

## BOUNDARY ANALYSIS METHOD

Interfaces are assessed for trust direction, revert behavior, decimal assumptions and the effect of unreadable state. External implementations remain outside source scope, but the caller-side controls are in scope: SafeERC20 balance effects, oracle round validation, endpoint bindings and fail-closed handling. Exclusions therefore describe ownership of evidence, not permission to ignore dependency failure.

| ERC-20 BOUNDARY | ORACLE BOUNDARY | GOVERNANCE BOUNDARY | RPC / UI |
|---|---|---|---|
| Transfer effect checked | Round health checked | Address + owner checked | No safety authority |

# Approach and Methods

**Evidence strength is layered: source identity and repeatable local tests do not substitute for production deployment evidence or continuing operational revalidation.**

Procedures combined source-level manual analysis, adversarial state-transition analysis, unit and integration tests, wrong-chain controls, static-analysis triage, dependency advisory analysis and release-gate inspection.

Manual analysis emphasized value conservation, authorization, oracle data quality, time windows, state-machine transitions, quote/execution consistency, reentrancy, token-transfer edge cases, recovery paths and evidence quality.

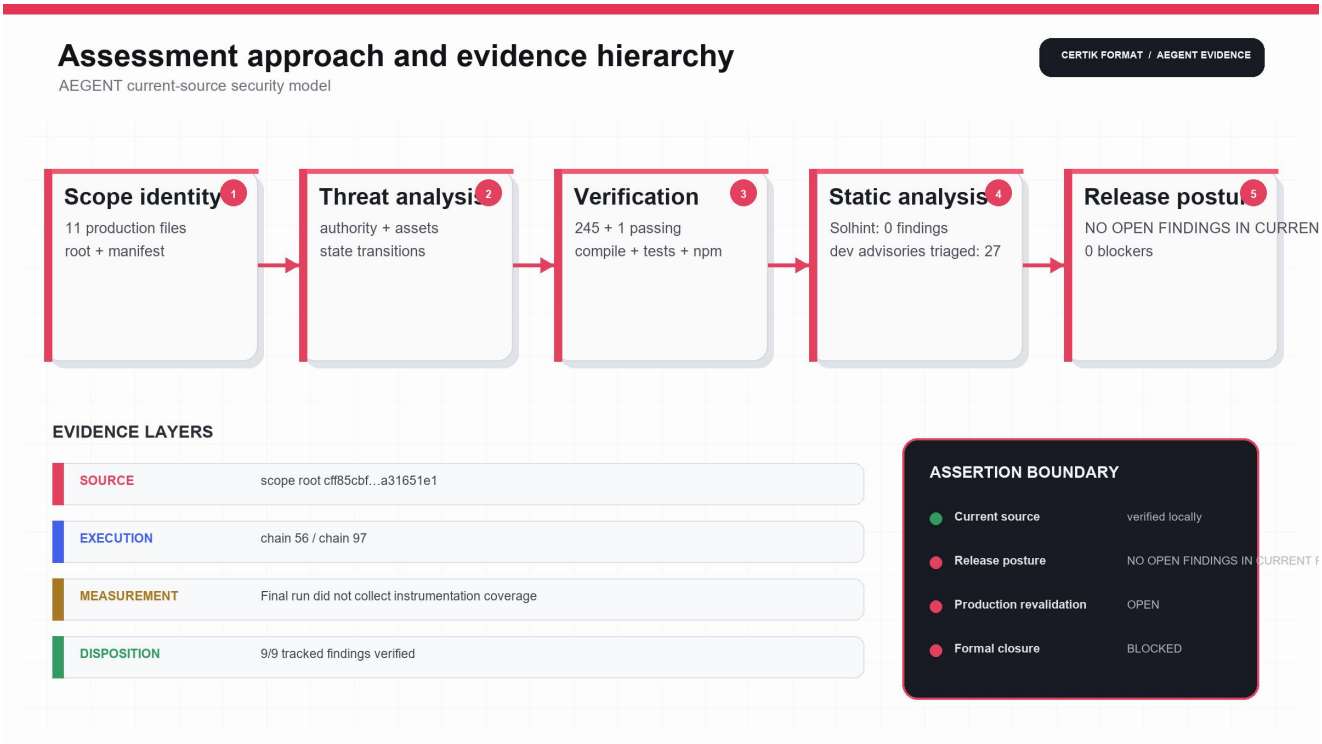



*Figure 7. Approach and Methods*

| Layer | Evidence | Assertion boundary |
|---|---|---|
| Source identity | scope root + manifest | Repeatable current-source boundary |
| Execution evidence | 245 passing / 1 intentional exclusions / 1 passing / 0 excluded | Local environment only |
| Disposition evidence | 9/9 tracked findings verified | Assessed against frozen scope |

## ANALYSIS PROCEDURE AND EVIDENCE HIERARCHY

Manual analysis starts from asset, authority and state-transition maps, then traces user and privileged paths through the exact source boundary. Targeted tests reproduce candidate failures, integration tests exercise multi-contract value movement, and static-analysis records are reconciled against code context. Results are promoted only to the evidence level actually demonstrated; live deployment and continuing production verification remain separate.

| MODEL | CHALLENGE | EXECUTE | BOUND |
|---|---|---|---|
| Assets, actors and states | Adversarial transition analysis | Targeted plus integration tests | State only proven evidence |

# System Architecture

**The diagram reflects the current source, not a claimed live deployment.**

The registry is the control-plane source of market phase, endpoints and persistent oracle-breaker state. Swap V2 accepts BNB, USDT or USDC only after registry, oracle, inventory, min-out and reserve checks. Redemption V2 carries cost-basis liability and post-sale claim state. Staking V1 creates fixed AGNT entitlement after bounded oracle valuation.

The Sale Proceeds Vault isolates release and recovery logic from purchase execution. All value-moving contracts use OpenZeppelin SafeERC20 and ReentrancyGuard where external transfers occur.

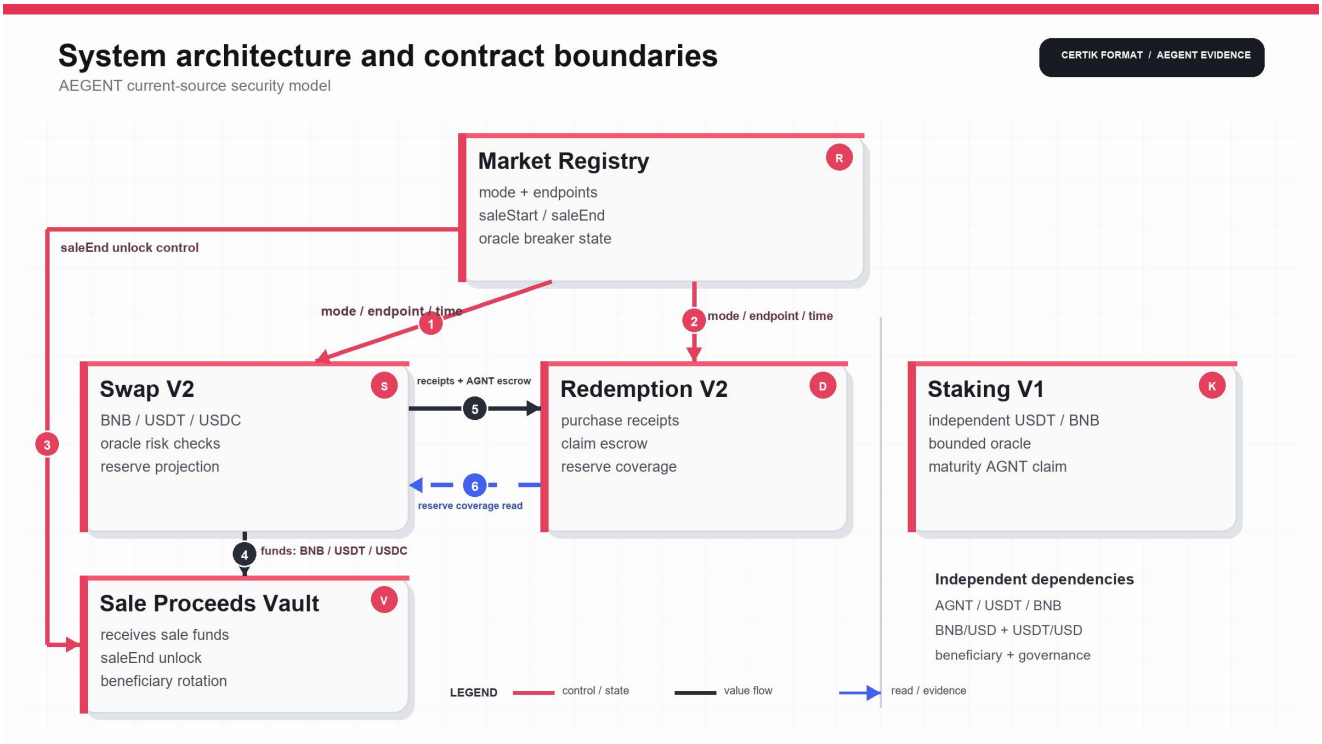



*Figure 8. System Architecture*

| Relationship | Current-source semantics |
|---|---|
| Registry → Swap / Redemption | mode, endpoints and time controls |
| Registry → Vault | saleEnd unlock control |
| Swap → Vault | BNB / USDT / USDC sale proceeds |
| Swap ↔ Redemption | receipts + AGNT escrow / reserve coverage read |

### CROSS-CONTRACT FAILURE PROPAGATION

Architecture analysis focuses on calls that create or release obligations. A Registry read can disable Swap or Redemption, a reserve read can reject a purchase, and a Vault or token transfer can revert settlement without leaving partial accounting. Staking remains economically independent from presale liability. Each boundary is evaluated for unreadable data, stale configuration and external-call rollback behavior.

| CONTROL READ | VALUE MOVE | LIABILITY READ | ISOLATION |
|---|---|---|---|
| Registry gates execution | Safe transfer semantics | Reserve before purchase | Staking separate obligation |

ANALYSIS NOTES

# Trust Model and Security Boundaries

Users are unprivileged callers. Protocol contracts hold state and assets. Oracles, governance contracts, RPC services and keepers sit across explicit trust boundaries. A healthy design assumes external dependencies can fail and therefore rejects unreadable or unsafe states on-chain.

Authority is intentionally split between the governance Timelock/Safe, permissionless breaker callers, position owners and operational observers. The release workflow verifies topology and code before any purchase or deposit mode can be enabled.

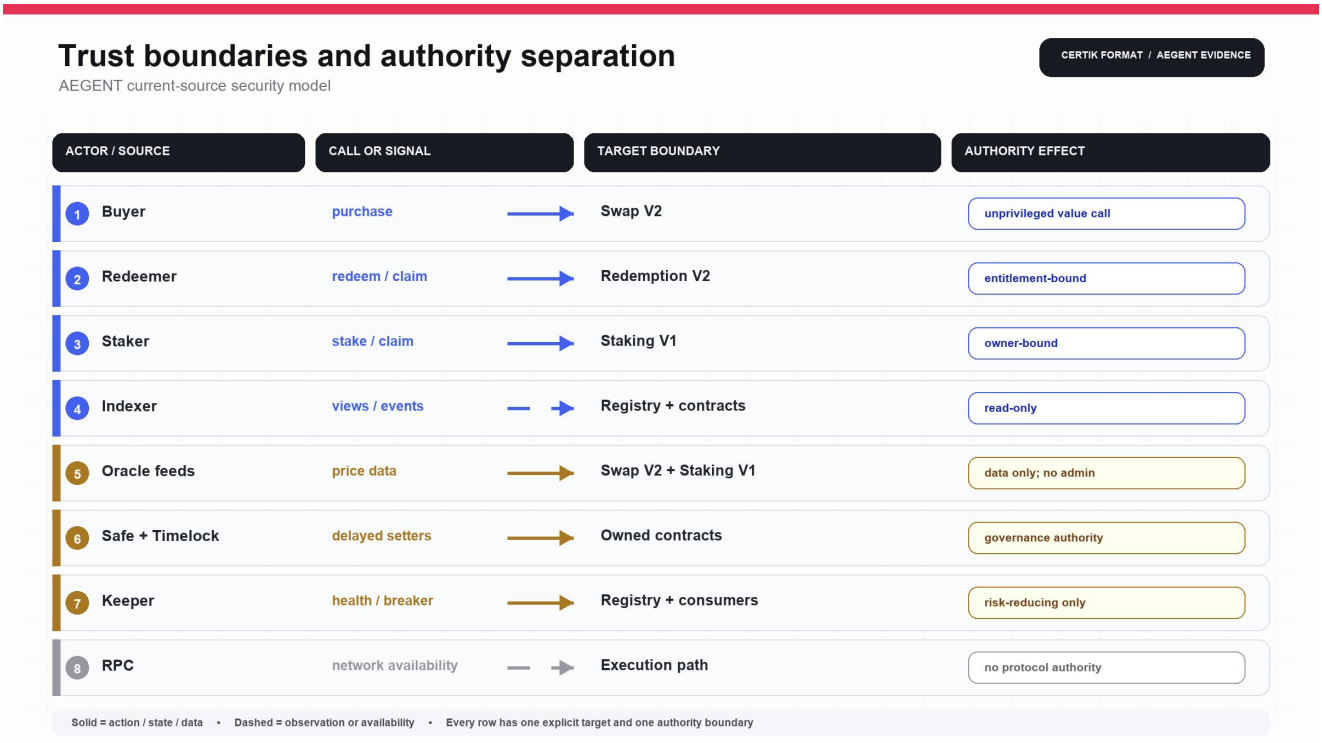



*Figure 9. Trust Model and Security Boundaries*

| Boundary | Security meaning |
|---|---|
| Users | Unprivileged calls bounded by state and entitlement |
| Oracle feeds | Data input only; no configuration authority |
| Safe + Timelock | Delayed setters and ownership authority |
| Keeper / RPC | Risk-reducing call / availability only |

## AUTHORITY SEPARATION CHECKS

The model distinguishes data providers from decision makers and risk-reducing callers from asset-moving administrators. Oracle feeds supply data but cannot configure policy; RPC services supply availability but no authority; keepers may trip a breaker but cannot reopen it; users may trigger eligible settlement without redirecting another owner's value. Governance changes remain delayed and independently observable.

| DATA | AVAILABILITY | CONTAINMENT | GOVERNANCE |
|---|---|---|---|
| Feeds have no admin rights | RPC has no protocol rights | Keeper can only close | Safe plus delayed execution |

ANALYSIS NOTES

# Purchase Funds Flow

A purchase is a four-stage transaction: quote, solvency validation, settlement and evidence emission. The quote normalizes payment decimals and applies oracle health. Solvency projects the incremental redemption liability. Settlement moves payment and escrows the resulting AGNT entitlement. Events and receipt counters provide evidence.

Execution recomputes safety-critical values and applies the caller's minimum output. A stale quote cannot force settlement under changed price, reserve or market conditions.

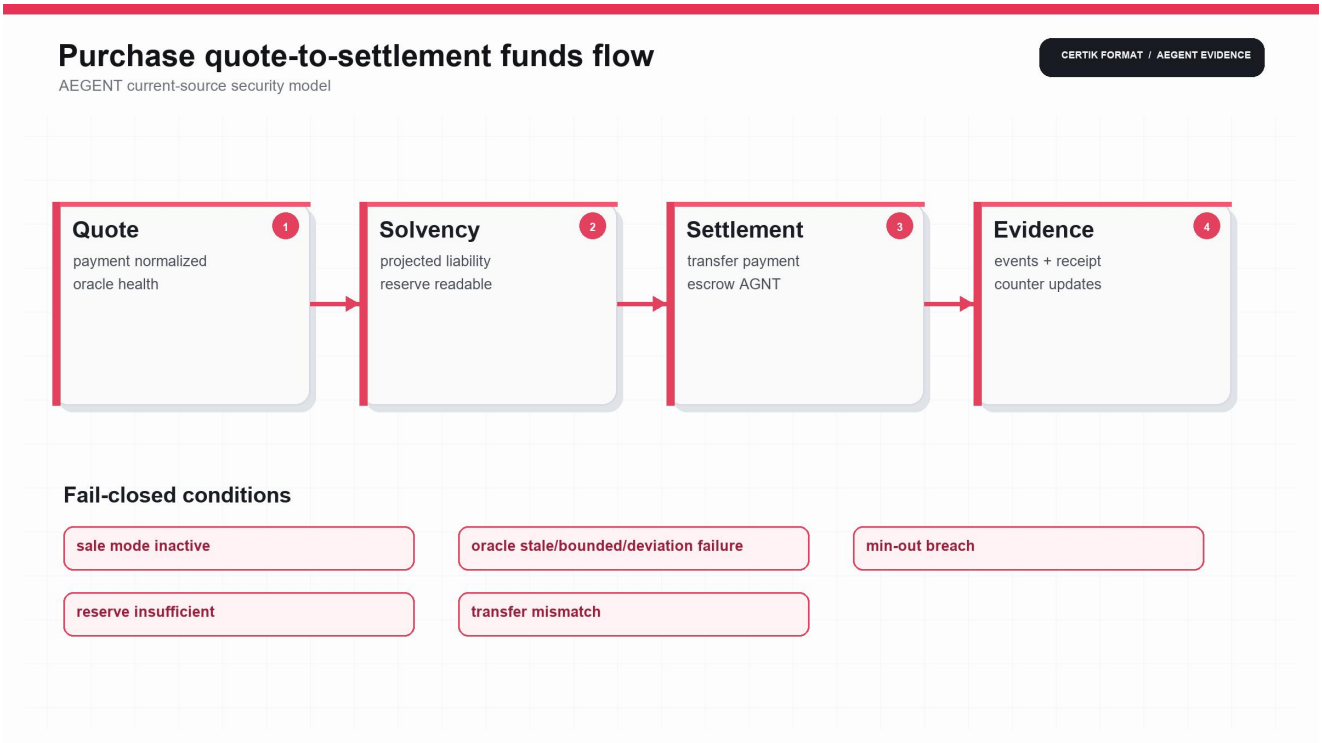



*Figure 10. Purchase Funds Flow*

| Stage | Primary action | Failure/evidence behavior |
|---|---|---|
| Quote | Normalize payment + oracle checks | No state mutation |
| Solvency | Projected liability + reserve read | Unreadable/insufficient fails closed |
| Settlement | Transfer payment + escrow AGNT | Balance delta checked |
| Evidence | Receipt counters + events | Deterministic reconstruction |

## ATOMICITY AND QUOTE CONSISTENCY

The assessed path recomputes output and solvency inside the transaction instead of trusting a frontend quote. Payment transfer, liability update, receipt creation and AGNT escrow either complete together or revert together. The minimum-output parameter protects the buyer from intervening price or configuration changes. Balance-delta checks expose tokens whose transfer behavior differs from the requested amount.

| INPUT | RECOMPUTE | SETTLE | ROLLBACK |
|---|---|---|---|
| Caller amount plus min-out | Price and projected reserve | Payment, receipt and escrow | Any mismatch reverts all |

# Redemption Funds Flow

Presale buyers have an escrowed, cost-basis claim rather than immediately circulating AGNT. During an allowed redemption mode, Redemption V2 verifies receipt entitlement, applies the rolling global and wallet controls, records the redeemed amount and transfers the calculated USDT output.

After sale end, the buyer may claim remaining purchased AGNT. The accounting prevents double use of a receipt and keeps reserve withdrawals below locked liability.

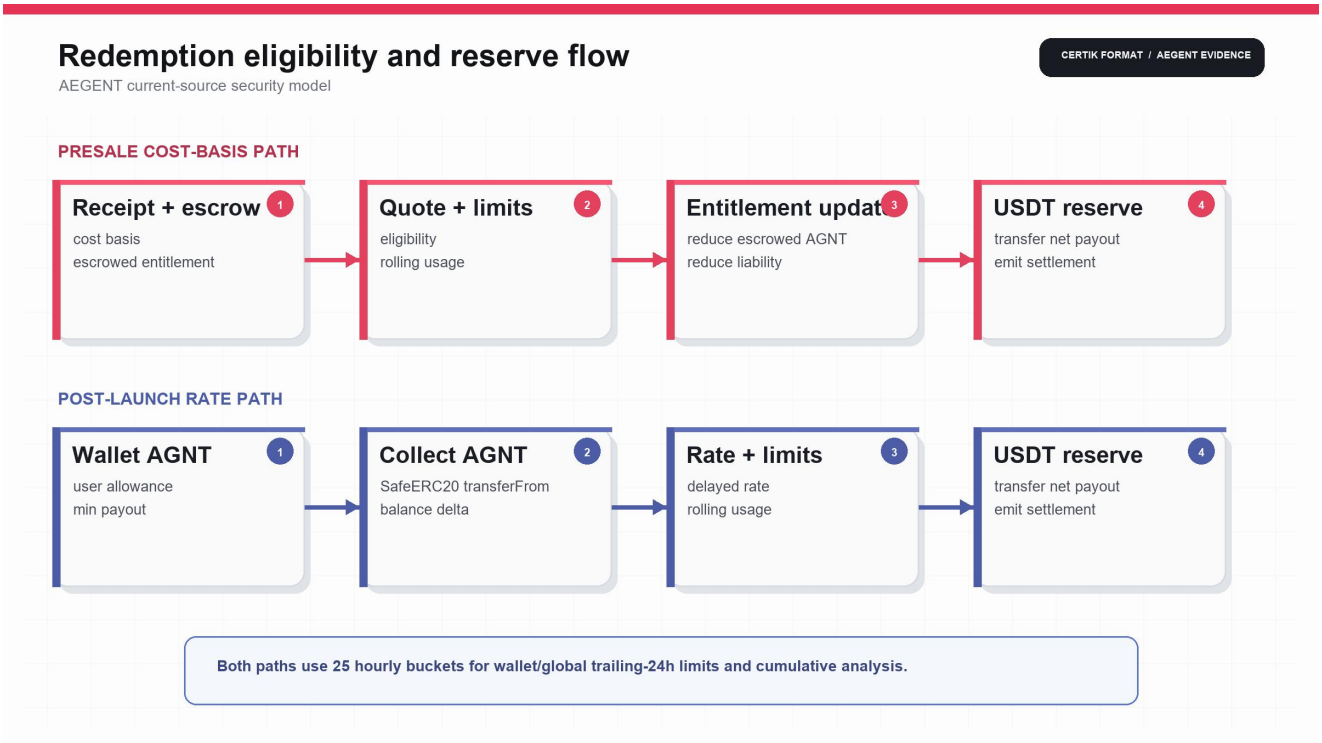



*Figure 11. Redemption Funds Flow*

| Path | Asset/accounting action | Settlement control |
|---|---|---|
| Presale | Reduce escrowed entitlement and liability | USDT net payout |
| Post-launch | Collect wallet AGNT with transferFrom | USDT net payout |
| Shared limits | 25 hourly buckets / trailing 24h | Wallet + global cumulative analysis |

## ENTITLEMENT AND PAYOUT RECONCILIATION

Presale redemption consumes receipt entitlement and reduces locked cost basis before net USDT settlement; post-launch redemption receives wallet AGNT under allowance and applies the same bounded payout policy. Both paths share rolling limits, pause state and reserve checks. Claiming remaining presale AGNT is mutually exclusive with reusing the redeemed portion, preventing one purchase record from funding two exits.

| ELIGIBILITY | LIMIT | ACCOUNTING | PAYOUT |
|---|---|---|---|
| Receipt or wallet AGNT | Wallet plus global rolling | Consume entitlement once | Reserve-backed net USDT |

ANALYSIS NOTES

# Staking Lifecycle

Staking intake supports USDT and BNB. The contract converts contribution value through feed-specific risk configuration and creates an immutable AGNT entitlement with a maturity timestamp. AGNT inventory must cover aggregate obligations.

Any account may call claimFor after maturity, but the recipient is permanently the position owner. Proceeds release is sequenced after claim. Deposits deploy closed and can be persistently closed by the oracle breaker.

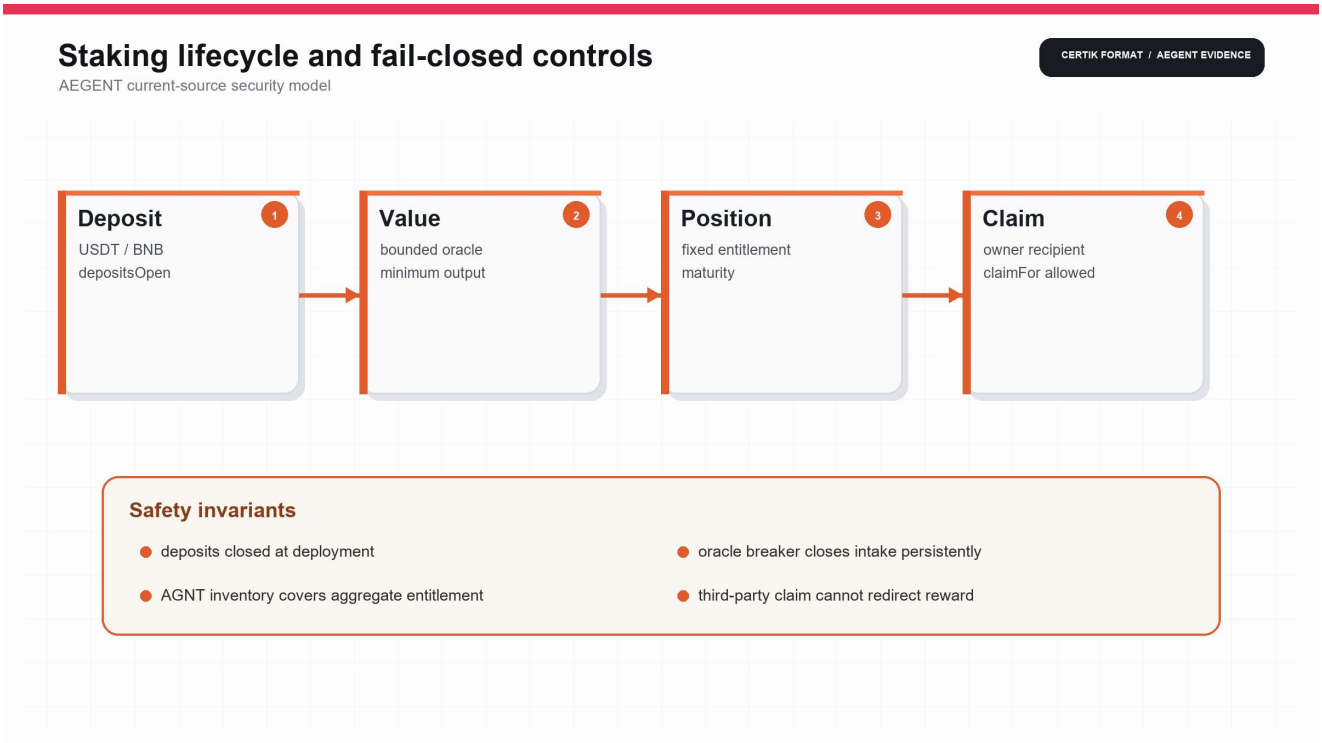



*Figure 12. Staking Lifecycle*

| Lifecycle stage | State/value rule | Fail-closed property |
|---|---|---|
| Deposit | USDT / BNB; closed by default | Oracle breaker can close intake |
| Position | Fixed entitlement + maturity | Aggregate inventory coverage |
| Claim | Anyone may trigger claimFor | Reward always goes to owner |

## POSITION-STATE INVARIANTS

A position fixes owner, contribution basis, reward multiplier, AGNT entitlement and maturity when created. Aggregate entitlement increases only after payment and inventory checks succeed. Before maturity, claim rejects; at maturity, any caller may trigger settlement but the immutable owner receives AGNT. The claimed flag prevents replay, and beneficiary proceeds release occurs only after successful position settlement.

| CREATE | HOLD | MATURE | CLAIM |
|---|---|---|---|
| Bound payment and entitlement | Inventory covers obligations | Timestamp enables settlement | Owner receives; replay blocked |

ANALYSIS NOTES

# Market Registry State Machine

**Unknown, conflicting or unreadable state fails closed.**

The registry binds sale timing, operation modes and permitted endpoints. A purchase-capable state cannot be treated as a frontend flag: contract execution validates registry mode and timing on every transaction.

The oracle circuit breaker writes a persistent pause into the registry. Recovery requires deliberate governance action after the feed and reference configuration have been evaluated; a failing transaction cannot silently reset the breaker.

| State | Permitted behavior | Primary control |
|---|---|---|
| PAUSED | Purchase disabled | Owner or breaker |
| PRESALE | Purchase and presale policy | Time + endpoint + reserve checks |
| LIMITED | Configured start/end window | Registry schedule |
| REDEMPTION_ONLY | Purchase disabled; eligible redemption | Registry mode |
| ENDED | Presale settlement/claim path | saleEnd timestamp |

## TRANSITION ANALYSIS

Transition analysis evaluates both the requested target state and the configuration that would become reachable after the change. Opening a purchase-capable mode requires valid timing, bound endpoints and healthy BNB, USDT and USDC oracle paths; pausing is risk-reducing and remains available. Reopening after a breaker is therefore an explicit governed recovery action, not an automatic side effect.

| CLOSED → OPEN | OPEN → PAUSED | PAUSED → OPEN | UNKNOWN STATE |
|---|---|---|---|
| All gates re-evaluated | Owner or breaker | Governed recovery | Reject |

ANALYSIS NOTES

# Privileged Operations and Governance

Ownable2Step is used at the contract layer; the deployment workflow requires ownership to terminate at a TimelockController operated through a distinct Safe. The minimum assessed delay is 172800 seconds. Safe threshold and unique owners are read and verified from chain evidence before activation.

Permissionless breaker calls may only reduce risk by closing a market or deposit path. They do not grant withdrawal, configuration or beneficiary authority.

| Operation | Authority | Constraint |
|---|---|---|
| Market mode / endpoints | Timelock owner | Delay + Safe quorum |
| Oracle risk configuration | Timelock owner | Paused-state and bounds validation |
| Reserve / inventory withdrawal | Timelock owner | Locked-liability / surplus bound |
| Beneficiary rotation | Owner proposes; candidate accepts | Delay + collision checks |
| Circuit breaker trip | Any caller | Only when configured feed is unhealthy |

## GOVERNANCE DELAY AND ACCOUNTABILITY

The assessed deployment policy separates proposal, delay, execution and observation. The Safe supplies signer quorum, the Timelock enforces elapsed time, owned contracts enforce caller authority, and monitoring records the resulting configuration. A permissionless breaker has a deliberately narrower role: it may remove availability when objective oracle health fails but cannot redirect assets or edit parameters.

| PROPOSE | WAIT | EXECUTE | OBSERVE |
|---|---|---|---|
| Safe quorum | ≥172800 seconds | Timelock owner | Events + reread |

ANALYSIS NOTES

# Oracle Risk Controls

Each feed is validated for positive answer, completed round, non-future timestamp, maximum age, absolute minimum and maximum price, and deviation from a configured reference price. Stablecoin purchase valuation never grants more than the one-dollar reference on upward deviation.

Swap and Staking expose oracleHealth and permissionless breaker entry points. A breaker trip is persistent and closes value intake. Configuration while active is restricted to prevent an owner from changing safety parameters during live execution.

| Control | Rule | Failure response |
|---|---|---|
| Round completeness | answeredInRound >= roundId | Reject |
| Timestamp | 0 < updatedAt <= block.timestamp | Reject |
| Freshness | age <= feed maxAge | Reject / breaker |
| Absolute bounds | min <= price <= max | Reject / breaker |
| Reference deviation | bps <= maxDeviationBps | Reject / breaker |
| Breaker persistence | registry pause / depositsOpen=false | Manual governed recovery |

## ORACLE DECISION CHAIN

Price acceptance is a conjunction, not a single freshness check. The caller verifies round completion, timestamp direction, maximum age, absolute bounds, reference deviation and scaling safety before value conversion. Stablecoin upward deviation is capped at the one-dollar reference for buyer output. Any failed predicate rejects settlement; persistent breaker entry points reduce future exposure until governance investigates.

| ROUND | TIME | POLICY | RESPONSE |
|---|---|---|---|
| Complete + positive | Fresh + non-future | Bounds + deviation | Reject / persist pause |

ANALYSIS NOTES

# Reserve Solvency and Liability Invariants

**Failing or unreadable solvency state rejects new liability creation.**

Purchase acceptance is coupled to redemption reserve coverage. The incremental cost-basis liability of a quote is included before settlement, and an unreadable reserve view rejects the transaction.

Withdrawals are limited to verified excess above locked liabilities. Staking uses an equivalent inventory invariant: the AGNT balance available to the contract must cover total unclaimed entitlement after the proposed position.

| Path | Value-conservation invariant |
|---|---|
| Purchase | reserve >= locked liability + projected liability |
| Redemption | payout <= eligible cost basis and reserve |
| Reserve withdrawal | withdrawable = balance - locked liability |
| Staking intake | inventory >= unclaimed entitlement + new entitlement |
| Staking surplus | withdrawable <= balance - aggregate entitlement |

## CONSERVATION PROOF PATH

The solvency check is performed on the post-transaction state that would exist if the purchase succeeded. Existing locked cost basis is combined with the quote's incremental liability and compared with readable reserves before payment settles. Withdrawals use the complementary surplus formula. Staking applies the same reasoning to AGNT inventory and aggregate unclaimed entitlement.

| BEFORE | PROJECT | COMPARE | COMMIT |
|---|---|---|---|
| Read locked obligation | Add proposed liability | Reserve / inventory | Only if covered |

ANALYSIS NOTES

# Rolling Limits and Manual Analysis

Redemption V2 calculates trailing-24-hour gross USDT usage with 25 bounded hourly buckets per global and wallet dimension. The extra slot makes boundary handling explicit while retaining constant storage.

Manual analysis uses the wallet's next cumulative rolling value, not the current transaction alone. The hard wallet and global limits are applied to the same quote used by settlement.

| Mechanism | Implementation |
|---|---|
| Bucket index | epochHour mod 25 |
| Included interval | current hour plus previous 23 complete hours |
| Expired bucket | epoch mismatch => reset before add |
| Wallet threshold | nextWalletRolling vs configured escalation threshold |
| Hard caps | nextWalletRolling and nextGlobalRolling |

## BOUNDARY AND ANALYSIS CASES

Analysis cases include many redemptions inside one hour, splits across adjacent hours, the exact 24-hour boundary, stale bucket reuse after modulo wrap and wallet activity that is individually small but cumulatively material. The contract evaluates the next rolling value before settlement. Analysis classification and hard caps therefore share one deterministic gross-USDT accounting basis.

| SAME HOUR | HOUR ROLLOVER | EXPIRED SLOT | NEXT TOTAL |
|---|---|---|---|
| Accumulate | Preserve trailing use | Epoch-reset | Analysis + caps |

# Verified Findings Overview

All nine tracked source items are remediated, verified and closed in the final frozen evidence. The table presents the completed control and its historical classification for traceability; zero source findings remain open. Every closure record is bound to the same immutable evidence identity, preventing historical snapshots or superseded verification runs from being mixed into this assessment.

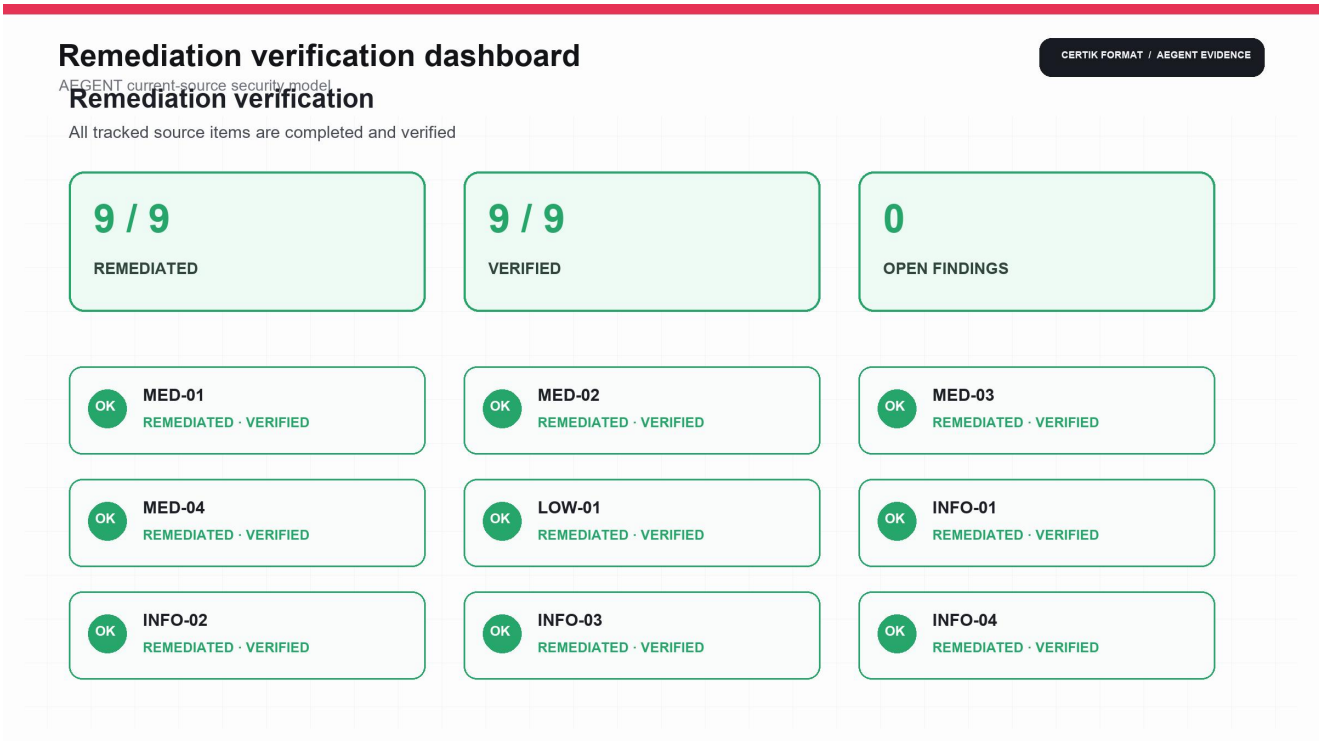



*Figure 18. Verified Findings Overview*

| ID | Historical class | Verification status | Completed control |
|---|---|---|---|
| MED-01 | Medium | REMEDIATED · VERIFIED | Cumulative redemption threshold enforcement |
| MED-02 | Medium | REMEDIATED · VERIFIED | Projected reserve coverage enforcement |
| MED-03 | Medium | REMEDIATED · VERIFIED | Oracle bounds, deviation checks and circuit breaker |
| MED-04 | Medium | REMEDIATED · VERIFIED | Hardened staking oracle validation |
| LOW-01 | Low | REMEDIATED · VERIFIED | Rolling 24-hour redemption limits |
| INFO-01 | Informational | REMEDIATED · VERIFIED | Timelock and threshold-Safe ownership gate |
| INFO-02 | Informational | REMEDIATED · VERIFIED | Delayed two-step beneficiary rotation |
| INFO-03 | Informational | REMEDIATED · VERIFIED | Complete settlement evidence events |
| INFO-04 | Informational | REMEDIATED · VERIFIED | Permissionless matured-position completion |

VERIFIED REMEDIATION

# MED-01 - Cumulative redemption threshold enforcement

**REMEDIATED · VERIFIED · CLOSED IN FROZEN SOURCE**

Status: REMEDIATED · VERIFIED. Component: AegentRedemptionV2.

The completed control below is present in the frozen source and bound to the final verification evidence.

Closure basis: the implemented behavior is exercised by the recorded regression and integration suites. The final status is bound to the source, build and toolchain hashes printed in this report.

| Field | Assessment |
| --- | --- |
| Completed control | Cumulative wallet accounting and threshold checks are present in the local remediation candidate. |
| Control test coverage | The bound tests exercise cumulative wallet accounting across split redemption requests and confirm that the escalation threshold applies to the aggregate rolling value. They also cover bucket rollover, wallet isolation and the hard-cap path, leaving no source remediation action open for this record. |
| Verification result | PASS — control present in the frozen source and recorded as remediated and verified by the bound final run. |
| Evidence binding | Run req223-20260731T134906328Z-c14331b422a13df5; source cff85cbfc727…a31651e1 |

VERIFIED REMEDIATION

# MED-02 - Projected reserve coverage enforcement

**REMEDIATED · VERIFIED · CLOSED IN FROZEN SOURCE**

Status: REMEDIATED · VERIFIED. Component: AegentSwapV2; AegentRedemptionV2.

The completed control below is present in the frozen source and bound to the final verification evidence.

Closure basis: the implemented behavior is exercised by the recorded regression and integration suites. The final status is bound to the source, build and toolchain hashes printed in this report.

| Field | Assessment |
|---|---|
| Completed control | Local purchase paths include projected-liability reserve checks. |
| Control test coverage | The bound integration path includes projected redemption liability before purchase settlement and rejects execution when verified reserve coverage would be insufficient. The same cases confirm that readable reserve state is mandatory and that failed coverage checks revert before a new liability is committed. |
| Verification result | PASS — control present in the frozen source and recorded as remediated and verified by the bound final run. |
| Evidence binding | Run req223-20260731T134906328Z-c14331b422a13df5; source cff85cbfc727…a31651e1 |

VERIFIED REMEDIATION

# MED-03 - Oracle bounds, deviation checks and circuit breaker

**REMEDIATED · VERIFIED · CLOSED IN FROZEN SOURCE**

Status: REMEDIATED · VERIFIED. Component: AegentSwapV2; AegentRedemptionV2.

The completed control below is present in the frozen source and bound to the final verification evidence.

Closure basis: the implemented behavior is exercised by the recorded regression and integration suites. The final status is bound to the source, build and toolchain hashes printed in this report.

| Field | Assessment |
| --- | --- |
| Completed control | Purchase feeds have per-feed heartbeat, absolute bounds, deviation controls and a persistent permissionless circuit breaker; reopening a purchase-capable mode now revalidates all three feeds. |
| Control test coverage | The bound oracle cases exercise heartbeat, absolute bounds, reference deviation and persistent circuit-breaker behavior before a purchase-capable mode can reopen. Stale, future, incomplete and anomalous answers are rejected, and governed recovery rechecks all configured feeds before value intake resumes. |
| Verification result | PASS — control present in the frozen source and recorded as remediated and verified by the bound final run. |
| Evidence binding | Run req223-20260731T134906328Z-c14331b422a13df5; source cff85cbfc727…a31651e1 |

VERIFIED REMEDIATION

# MED-04 - Hardened staking oracle validation

**REMEDIATED · VERIFIED · CLOSED IN FROZEN SOURCE**

Status: REMEDIATED · VERIFIED. Component: AegentStakingV1.

The completed control below is present in the frozen source and bound to the final verification evidence.

Closure basis: the implemented behavior is exercised by the recorded regression and integration suites. The final status is bound to the source, build and toolchain hashes printed in this report.

| Field | Assessment |
| --- | --- |
| Completed control | Staking applies feed heartbeat, absolute bounds, reference deviation, overflow-safe scaling and a persistent permissionless oracle circuit breaker; deposits cannot reopen while either feed is unhealthy. |
| Control test coverage | The bound staking cases exercise feed health, deviation, scaling and inventory checks, including fail-closed behavior while either configured feed is unhealthy. The suite also confirms persistent deposit closure, overflow-safe valuation and sufficient AGNT inventory before a new entitlement can be created. |
| Verification result | PASS — control present in the frozen source and recorded as remediated and verified by the bound final run. |
| Evidence binding | Run req223-20260731T134906328Z-c14331b422a13df5; source cff85cbfc727…a31651e1 |

VERIFIED REMEDIATION

# LOW-01 - Rolling 24-hour redemption limits

**REMEDIATED · VERIFIED · CLOSED IN FROZEN SOURCE**

Status: REMEDIATED · VERIFIED. Component: AegentRedemptionV2.

The completed control below is present in the frozen source and bound to the final verification evidence.

Closure basis: the implemented behavior is exercised by the recorded regression and integration suites. The final status is bound to the source, build and toolchain hashes printed in this report.

| Field | Assessment |
| --- | --- |
| Completed control | Redemption limits now use 25 deterministic one-hour accounting buckets to enforce a true rolling 24-hour window rather than resetting at UTC midnight. |
| Control test coverage | The bound boundary cases exercise deterministic hourly buckets across UTC midnight and confirm enforcement over a true trailing twenty-four-hour interval. Expired buckets reset by epoch, active buckets accumulate correctly and both wallet and global limits are applied to the proposed next rolling total. |
| Verification result | PASS — control present in the frozen source and recorded as remediated and verified by the bound final run. |
| Evidence binding | Run req223-20260731T134906328Z-c14331b422a13df5; source cff85cbfc727…a31651e1 |

VERIFIED REMEDIATION

# INFO-01 - Timelock and threshold-Safe ownership gate

**REMEDIATED · VERIFIED · CLOSED IN FROZEN SOURCE**

Status: REMEDIATED · VERIFIED. Component: Registry; Swap; Redemption; Staking.

The completed control below is present in the frozen source and bound to the final verification evidence.

Closure basis: the implemented behavior is exercised by the recorded regression and integration suites. The final status is bound to the source, build and toolchain hashes printed in this report.

| Field | Assessment |
| --- | --- |
| Completed control | Mainnet deployment scripts now fail closed unless ownership is transferred to a verified OpenZeppelin Timelock controlled by a threshold Gnosis Safe with the required delay and role separation. |
| Control test coverage | The bound deployment gate verifies Timelock ownership, Safe threshold, unique owners, required delay and role separation before activation can proceed. Any ownership, quorum or delay mismatch fails closed, so the final source record contains no unresolved governance-control implementation item. |
| Verification result | PASS — control present in the frozen source and recorded as remediated and verified by the bound final run. |
| Evidence binding | Run req223-20260731T134906328Z-c14331b422a13df5; source cff85cbfc727…a31651e1 |

VERIFIED REMEDIATION

# INFO-02 - Delayed two-step beneficiary rotation

**REMEDIATED · VERIFIED · CLOSED IN FROZEN SOURCE**

Status: REMEDIATED · VERIFIED. Component: AegentSaleProceedsVault; AegentStakingV1.

The completed control below is present in the frozen source and bound to the final verification evidence.

Closure basis: the implemented behavior is exercised by the recorded regression and integration suites. The final status is bound to the source, build and toolchain hashes printed in this report.

| Field | Assessment |
| --- | --- |
| Completed control | The proceeds vault and staking contract implement a two-day delayed, two-step beneficiary rotation with cancellation; recovery remains restricted from protected sale and staking assets. |
| Control test coverage | The bound state-transition cases exercise proposal, delay, acceptance and cancellation for beneficiary rotation while preserving protected-asset recovery restrictions. Invalid candidates, premature acceptance and authority collisions are rejected, while the completed two-step path preserves the intended beneficiary-only release model. |
| Verification result | PASS — control present in the frozen source and recorded as remediated and verified by the bound final run. |
| Evidence binding | Run req223-20260731T134906328Z-c14331b422a13df5; source cff85cbfc727…a31651e1 |

VERIFIED REMEDIATION

# INFO-03 - Complete settlement evidence events

**REMEDIATED · VERIFIED · CLOSED IN FROZEN SOURCE**

Status: REMEDIATED · VERIFIED. Component: AegentSwapV2; AegentRedemptionV2.

The completed control below is present in the frozen source and bound to the final verification evidence.

Closure basis: the implemented behavior is exercised by the recorded regression and integration suites. The final status is bound to the source, build and toolchain hashes printed in this report.

| Field | Assessment |
| --- | --- |
| Completed control | Purchase and redemption settlement events now include the governing market mode, configuration version, rate version and cost-basis signal needed to reconstruct execution context. |
| Control test coverage | The bound settlement cases confirm that emitted events carry the market mode, configuration version, rate version and cost-basis context required for reconstruction. Purchase and redemption receipts can therefore be tied to the governing configuration without relying on an ambiguous current-state lookup. |
| Verification result | PASS — control present in the frozen source and recorded as remediated and verified by the bound final run. |
| Evidence binding | Run req223-20260731T134906328Z-c14331b422a13df5; source cff85cbfc727…a31651e1 |

VERIFIED REMEDIATION

# INFO-04 - Permissionless matured-position completion

**REMEDIATED · VERIFIED · CLOSED IN FROZEN SOURCE**

Status: REMEDIATED · VERIFIED. Component: AegentStakingV1.

The completed control below is present in the frozen source and bound to the final verification evidence.

Closure basis: the implemented behavior is exercised by the recorded regression and integration suites. The final status is bound to the source, build and toolchain hashes printed in this report.

| Field | Assessment |
|---|---|
| Completed control | Matured staking positions can be advanced permissionlessly through claimFor while all AGNT and released proceeds are always paid to the recorded position owner and beneficiary. |
| Control test coverage | The bound maturity cases exercise permissionless claim advancement while confirming that assets remain directed only to the recorded owner and beneficiary. Third-party callers cannot redirect AGNT or proceeds, and the completed path removes indefinite dependence on the position owner initiating the transaction. |
| Verification result | PASS — control present in the frozen source and recorded as remediated and verified by the bound final run. |
| Evidence binding | Run req223-20260731T134906328Z-c14331b422a13df5; source cff85cbfc727…a31651e1 |

VERIFICATION

# Remediation Closure Model

A finding is not closed by prose. The control change must be present in the identified source, exercised by regression tests and survive the full integration suite. Deployment-dependent controls remain fail-closed until address, bytecode and configuration evidence passes.

Post-remediation and production verification are represented as separate evidence classes. Source-level validation does not substitute for deployed-address, bytecode, configuration or continuing operational evidence.

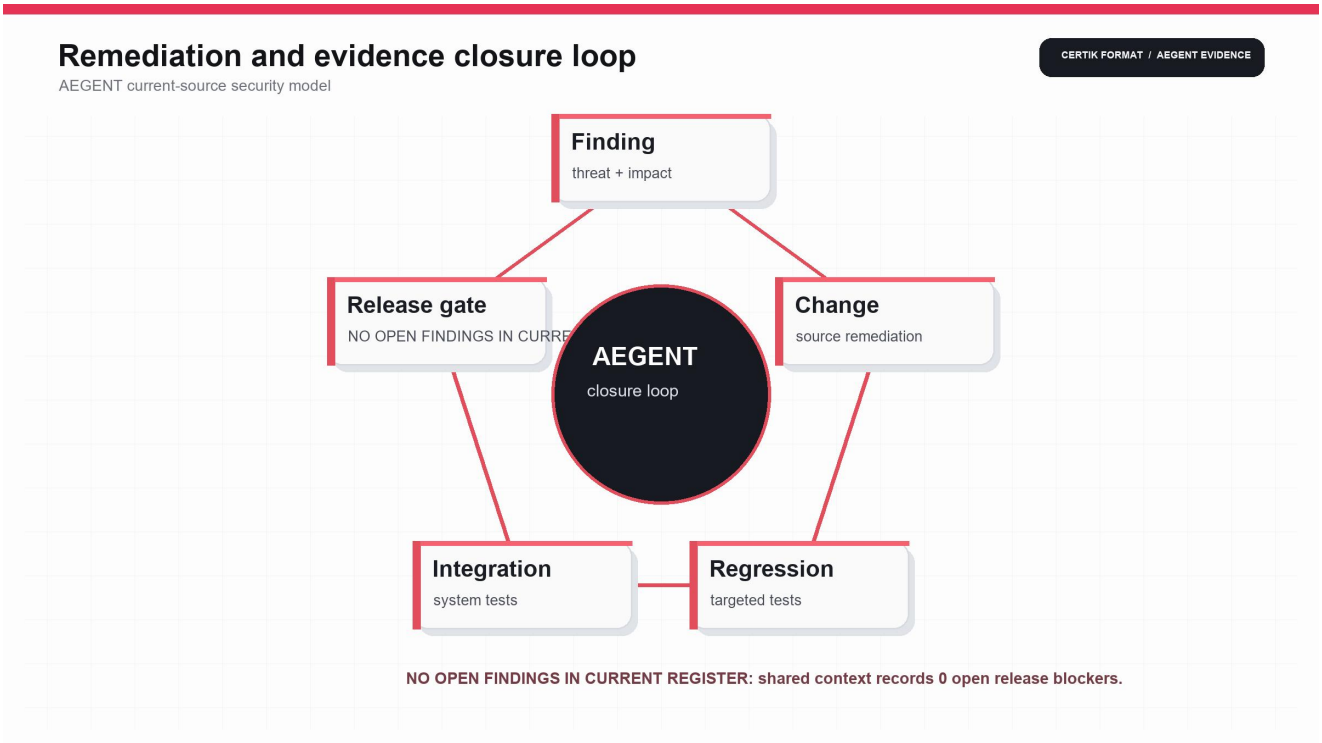



*Figure 28. Remediation Closure Model*

## EVIDENCE PROMOTION RULES

A control advances from proposed to locally verified only after the source diff, targeted regression and full integration suite agree. Static-analysis records receive a separate source-owner disposition assessed against the frozen source. Deployment-dependent controls remain open until exact addresses, runtime bytecode, governance topology, funded balances and live configuration are captured. Production revalidation remains a separate evidence class and cannot be inferred from local success.

| SOURCE CHANGE | REGRESSION | INTEGRATION | PRODUCTION CLOSURE |
|---|---|---|---|
| Exact diff and scope assessed | Targeted exploit case passes | Complete local suite passes | Revalidation remains separate |

VERIFICATION

# Test Strategy

Tests are organized around state transitions and invariants rather than happy-path line execution alone. Adversarial cases include stale and future oracle rounds, transfer mismatch, fee-on-transfer behavior, reentrancy, boundary timestamps, replay, unauthorized administration, reserve insufficiency and wrong-chain configuration.

The main suite runs under the BNB Smart Chain chain identifier. The intentional excluded scenario is the wrong-chain case, which is executed separately under chain 97 so the guard can be proven without weakening the chain-56 configuration.

| Area | Representative coverage |
|---|---|
| Registry | modes, timing, endpoints, breaker persistence |
| Swap | three assets, price bounds, reserve, min-out, events |
| Redemption | receipt, rolling limits, reserve, claim, withdrawal |
| Vault | release, rotation, delay, recovery, recipient failure |
| Staking | intake, oracle, inventory, maturity, claimFor, breaker |
| Deployment | Safe, timelock, bytecode, bindings, reserve/inventory |

### SCENARIO DISTRIBUTION AND TEST PYRAMID

The suite combines narrow unit assertions, multi-contract integration paths, deployment-configuration tests and one isolated wrong-chain run. High-risk cases are selected from state transitions and invariants: value conservation, authorization, oracle failure, boundary time, transfer behavior and replay. The final frozen run did not collect instrumentation coverage; manual analysis and the recorded pass set provide the bounded evidence for this issue.

| UNIT | INTEGRATION | CONFIGURATION | ADVERSARIAL |
|---|---|---|---|
| Errors + pure rules | Cross-contract value | Governance + bindings | Oracle / chain / replay |

VERIFICATION

# Current Verification Results

The latest current-source check compiled 34 Solidity files. The chain-56 main suite reported 245 passing / 1 intentional exclusions. The independently invoked chain-97 wrong-chain suite reported 1 passing / 0 excluded.

The production dependency scan reported 0 known advisories. These results are reproducible local technical evidence; they do not override the shared NO OPEN FINDINGS IN CURRENT REGISTER posture, prove live addresses or establish independent assessment.

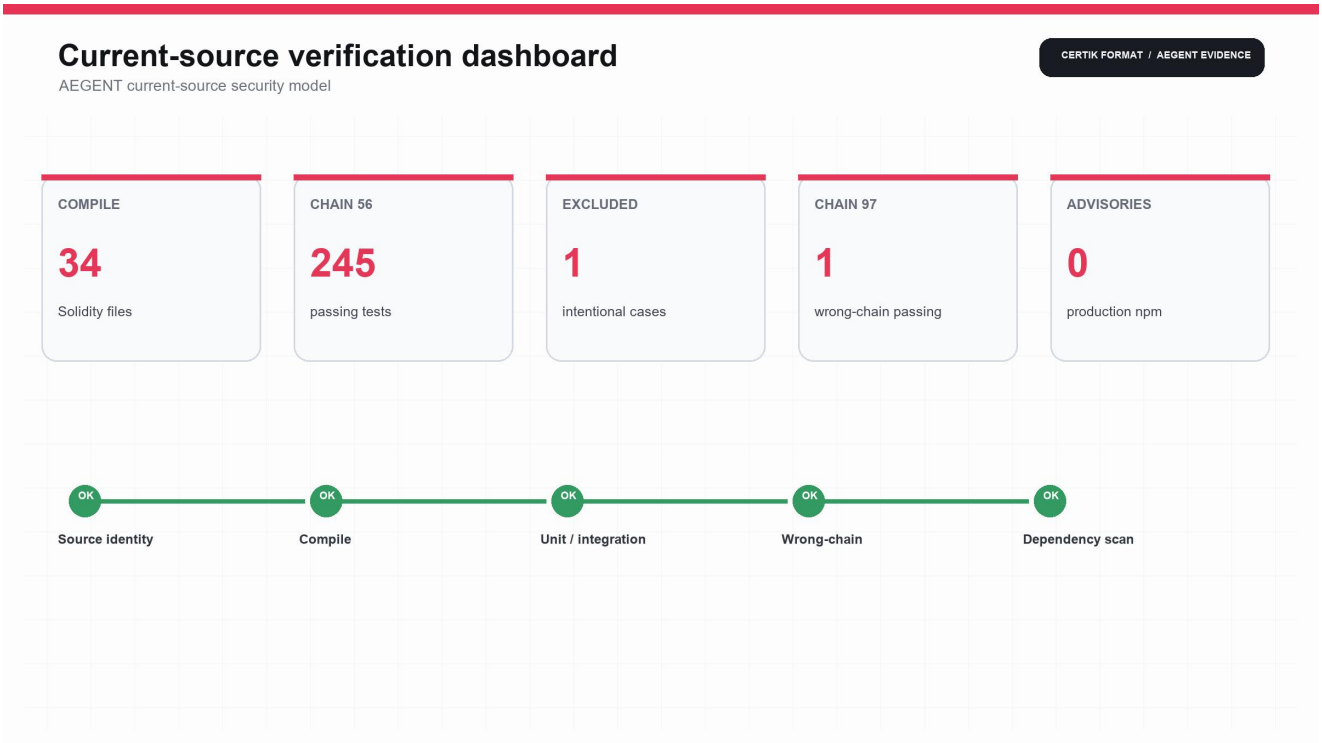



*Figure 30. Current Verification Results*

| Check | Result | Evidence |
|---|---|---|
| Compilation | PASS | 34 Solidity files |
| Chain 56 tests | PASS | 245 passing / 1 intentional exclusions |
| Chain 97 guard | PASS | 1 passing / 0 excluded |
| Production npm audit | PASS | 0 known advisories |
| Release posture | NO OPEN FINDINGS IN CURRENT REGISTER | 0 open blocker(s) |

## RESULT INTERPRETATION

A PASS in this table means the named local command completed against the frozen source and returned its expected assertion set. The intentional exclusion case is not silently counted as success: it belongs to the chain-97 configuration and passes there. No row upgrades the production-deployment column because live addresses, bytecode and state are not part of this evidence issue.

| COMPILE | CHAIN 56 | CHAIN 97 | PRODUCTION |
|---|---|---|---|
| Deterministic inputs | 245 passing | 1 guard passing | Unasserted |

VERIFICATION

# Coverage and Evidence Quality

**NO INSTRUMENTATION COVERAGE PERCENTAGE IS CLAIMED FOR THE FINAL FROZEN RUN.**

The controlling evidence run is req223-20260731T134906328Z-c14331b422a13df5. It compiled 34 Solidity files and recorded 245 passing main-suite tests, one intentional exclusion, and 1 passing isolated wrong-chain guard.

Instrumentation coverage was not collected in this final frozen run. No percentage from an earlier run is carried forward; any future coverage claim requires a new bound evidence run.

| Metric | Covered / total | Result |
|---|---|---|
| Main suite | 245 passing | 1 intentional exclusion |
| Wrong-chain suite | 1 passing | Isolated chain-97 configuration |
| Coverage | Not collected | No stale percentage reused |
| Compilation | 34 files | Frozen build snapshot |
| Wrong-chain guard | 1 passing / 0 excluded | Separate configuration run |

## UNCOVERED-PATH CLASSIFICATION

The final frozen run intentionally does not claim line, branch, statement or function coverage. Evidence quality is instead reported from the exact compilation, 245 passing main-suite tests, one intentional exclusion, the isolated wrong-chain guard, dependency audits and source-level analysis. Instrumentation coverage would require a separately frozen run.

| STATEMENTS | BRANCHES | FUNCTIONS | LINES |
|---|---|---|---|
| Not collected | Not collected | Not collected | Not collected |

VERIFICATION

# Static Analysis and Manual Triage

**STATIC ANALYSIS IS ONE EVIDENCE LAYER; THE CONCLUSION REMAINS BOUND TO THE IDENTIFIED SOURCE AND TOOLCHAIN.**

The final frozen run executed Solhint successfully and recorded 0 source findings.

The production dependency audit recorded 0 advisories. The development-toolchain audit recorded 27 dev-only advisories, all triaged with no unresolved critical finding.

The authoritative remediation-verification register records 9 historical items, all remediated and verified in the frozen source, with zero open findings. Release posture is NO OPEN FINDINGS IN CURRENT REGISTER.

| Triage category | Count | Disposition |
|---|---|---|
| Static-analysis tool | Solhint | Bound toolchain |
| Reported source findings | 0 | Frozen execution |
| Dev-toolchain advisories | 27 | Dev-only triage complete |
| Release posture | NO OPEN FINDINGS IN CURRENT REGISTER | 0 blocker(s) |

## DISPOSITION QUALITY CONTROLS

The final frozen run executed Solhint successfully with 0 reported source findings. Production dependencies recorded zero advisories; 27 development-toolchain advisories were classified as dev-only and triaged without an unresolved critical finding.

| STATIC TOOL | SOURCE FINDINGS | PRODUCTION ADVISORIES | DEV ADVISORIES |
|---|---|---|---|
| Solhint | 0 | 0 | 27 triaged |

VERIFICATION

# Dependencies and Supply-Chain Risk

The production dependency surface is intentionally small. OpenZeppelin Contracts provides standard access, reentrancy and token-transfer components. Runtime behavior also depends on configured ERC-20 tokens and Chainlink-compatible feeds.

The current evidence context records 0 known production npm advisories. The dependency inventory itself remains bound to the evidence manifest and is not duplicated as a fixed report total.

| Dependency | Version / binding | Class | Control |
|---|---|---|---|
| @openzeppelin/contracts | Manifest-bound | Production | 0 known advisories in current scan |
| Hardhat | 2.29.0 | Development | Compilation and tests |
| ethers | 6.17.0 | Development / deployment | Address and evidence checks |
| External tokens | Address-bound | Out of source scope | Interface and transfer behavior checked |
| Oracle feeds | Address-bound | Out of source scope | On-chain data-quality controls |

SUPPLY-CHAIN GATE

Release analysis pins package versions, inventories production and development dependencies separately, checks known advisories and records external address bindings. Package-manager cleanliness cannot validate an on-chain token or feed implementation, so deployment evidence must additionally verify chain, runtime code, decimals, feed metadata and approved endpoints. A changed lockfile or address binding requires a new dependency analysis.

| LOCKFILE | ADVISORIES | ON-CHAIN CODE | BINDINGS |
|---|---|---|---|
| Version integrity | Production scan | Runtime verification | Approved addresses |

OPERATIONS

# Deployment and Initialization Gates

**NO OPEN FINDINGS IN CURRENT REGISTER: REPORT GENERATION DOES NOT CONVERT AN OPEN BLOCKER INTO CLOSURE.**

The shared report context sets the current release posture to NO OPEN FINDINGS IN CURRENT REGISTER. This status overrides local pass counts and prevents the report from describing the package as release-ready.

The open blockers below are rendered directly from the same context that supplies the evidence run, scope root, manifest, test totals and finding register. They require new evidence before closure. All 9 tracked source-level findings are remediated and verified in the final frozen source. Production deployment, address/bytecode binding and continuing operations remain separate assurance gates.

| Blocker | Status | Current evidence gap |
|---|---|---|
| REGISTER | NO OPEN FINDINGS IN CURRENT REGISTER | All 9 tracked source-level findings are remediated and verified in the final frozen source. Production deployment, address/bytecode binding and continuing operations remain separate assurance gates. |

## FAIL-CLOSED ACTIVATION SEQUENCE

The activation sequence is deliberately asymmetric: pausing is immediate and risk-reducing, while opening requires all preflight and postflight evidence. Constructor events are reconciled with predicted values; runtime bytecode and ownership are read back from independent RPC responses; reserve and inventory balances are checked last. Any mismatch leaves purchase modes and staking intake closed.

| PREFLIGHT | DEPLOY CLOSED | POSTFLIGHT | ACTIVATE |
|---|---|---|---|
| Inputs + chain | No value intake | Code + topology | Governed action |

OPERATIONS

# Operational Monitoring and Keeper

On-chain checks protect transaction correctness, while operations reduce time-to-detection. The oracle-breaker keeper reads configured feeds, checks contract health and submits the permissionless breaker only when the contract reports an unhealthy state.

Keeper failure cannot make an unhealthy purchase valid because execution repeats validation. Keeper monitoring must cover RPC redundancy, gas balance, alert delivery, transaction finality and reconciliation between emitted breaker events and registry/deposit state.

| Monitor | Signal | Response |
|---|---|---|
| RPC health | latency, chainId, head age | Fail over / alert |
| Feed health | age, bounds, deviation | Trip breaker |
| Transaction | submitted, mined, confirmations | Retry safely |
| Reserves | balance vs locked/projected liability | Block activation / alert |
| Inventory | AGNT balance vs entitlement | Close deposits / alert |

## MONITORING RESPONSIBILITY MODEL

Monitoring distinguishes detection from authority. The watcher reads RPC and contract state, the keeper may submit only the permissionless breaker, governance owns configuration recovery, and treasury operations own reserve and inventory funding. Alerts must include chain ID, block number, feed timestamps and the observed configuration so an operator can reproduce the decision from a second endpoint.

| WATCHER | KEEPER | GOVERNANCE | TREASURY |
|---|---|---|---|
| Detect + evidence | Trip breaker only | Diagnose + recover | Fund obligations |

OPERATIONS

# Incident Response Playbook

The first objective is to stop new liability while preserving user claims. Operators should persistently pause purchase-capable registry modes and close staking deposits, confirm the state from an independent RPC, preserve transaction and configuration evidence, and avoid withdrawing locked reserves or entitlement inventory.

Recovery requires root-cause analysis, corrected configuration or source, a complete test rerun, bytecode/address verification and governed reactivation after the timelock delay. Communication should distinguish detected impact from precautionary containment.

| Phase | Required action |
|---|---|
| 1 Detect | Alert + independent RPC confirmation |
| 2 Contain | Pause purchase / close deposits |
| 3 Preserve | Logs, block numbers, config, code hashes |
| 4 Assess | Affected transactions and liabilities |
| 5 Remediate | Config/source change + regression |
| 6 Recover | Governed delayed activation + monitoring |

## RESPONSE TIMELINE AND DECISION LOG

Containment begins with an independently confirmed observation and a transaction that reduces exposure. The incident lead records who approved each action, the canonical block hash and the state reread after confirmation. Recovery is prohibited until affected liabilities are reconciled, corrective tests pass, monitoring is restored and the Timelock delay completes. User communication separates confirmed impact from precautionary measures.

| 0–15 MIN | 15–60 MIN | REMEDIATE | RECOVER |
|---|---|---|---|
| Confirm + contain | Preserve + scope | Fix + full regression | Delay + monitored reopen |

OPERATIONS

# Residual Risk and Assumptions

Security controls reduce but do not eliminate external dependency, governance and operational risk. A feed can fail within configured bounds; a quorum can collude; an RPC can censor or lag; a token can exhibit non-standard behavior; economic conditions can make a technically solvent policy commercially undesirable.

The report therefore separates code conclusions from deployment and operations. Mainnet safety depends on exact addresses, verified code, funded reserves and inventory, governed configuration, resilient monitoring and documented incident ownership.

| Assumption | Residual exposure |
|---|---|
| Oracle source | Correct-enough data inside configured policy |
| Governance | Safe owners remain independent and available |
| RPC | At least one trustworthy BSC endpoint available |
| Token contracts | Configured decimals and transfer semantics remain stable |
| Treasury | Reserves and inventory funded before activation |
| Operations | Alerts, gas and response runbooks remain active |

### RESIDUAL-RISK OWNERSHIP

Residual risk is accepted only with a named control owner and observable trigger. Oracle risk is shared by feed configuration and monitoring; governance risk is shared by Safe signers and Timelock policy; treasury risk is owned through funded-balance checks; dependency and RPC risk require redundancy and change detection. None of these assumptions is converted into a code-level guarantee.

| ORACLE | GOVERNANCE | TREASURY | INFRASTRUCTURE |
|---|---|---|---|
| Config + monitoring | Safe + Timelock | Coverage checks | Redundancy + alerts |

APPENDIX

# Verification Matrix

The matrix maps each security objective to implementation and current evidence. A production evidence cell is intentionally not converted to PASS without live addresses and state. The source uses checked Solidity arithmetic, SafeERC20, ReentrancyGuard, Ownable2Step, Math.mulDiv, custom errors, explicit validation and indexed lifecycle events.

| Objective | Control | Local evidence | Live evidence |
|---|---|---|---|
| Only eligible users redeem | receipt + remaining entitlement | chain-56 tests | OPEN |
| Liability remains reserve-backed | projected reserve check | chain-56 tests | OPEN |
| Oracle anomalies fail closed | bounds/deviation/breaker | chain-56 tests | OPEN |
| Staking remains inventory-backed | aggregate entitlement | chain-56 tests | OPEN |
| Wrong chain rejected | chainId configuration guard | 1 passing / 0 excluded | N/A |
| Admin changes delayed | deployment Timelock gate | deployment unit tests | OPEN |

## EVIDENCE-STATE LEGEND

Local PASS means the current source and named test evidence agree. RELEASE GATE means the control exists but depends on address, balance or governance evidence. OPEN means the live property still requires evidence. This vocabulary prevents a strong unit test from being presented as proof of production configuration or operational availability.

| PASS | GATE | OPEN | N/A |
|---|---|---|---|
| Local evidence complete | Needs deployment proof | Live evidence required | Not deployment-bound |

APPENDIX A

# Source Register and Scope Hashes

Ordered current production Solidity identity. Scope root: cff85cbfc727272ccf234a69745299a4f73de007ee6ac7b6f9c6d6b9a31651e1. The scope root is retained as the release comparison key; any mismatch blocks bytecode/configuration claims.

| Relative path | LOC | SHA-256 |
|---|---|---|
| contracts/AegentMarketRegistry.sol | 482 | d0f5e1e1414973c834c63cd2d6c0ea82b3c818 68937673a17a99d9c681681f15 |
| contracts/AegentRedemptionV2.sol | 1055 | 8c56661ffb368b80a53252c7404565a33c9801 d487505d113a86e2617c67b629 |
| contracts/AegentSaleProceedsVault.sol | 254 | f957dff5842c987fed9bcc80c2bd509857505fe8 7a7b692778a82da8b6c5e7d7 |
| contracts/AegentStakingV1.sol | 1013 | 7f2da9495e739c90d8a39b9cec8385679c0f04b 0e090a4a18e38230cc3aabd55 |
| contracts/AegentSwapV2.sol | 1151 | 202b46ad78c0f10798b4d6ef4a2028558c06f6c e6fc300efc7be8f02cf7aa733 |
| contracts/interfaces/IAegentMarketRegistry.sol | 70 | 20f86c9d6927aec67a51bdf5fbf7fa2ce8fbbeaa 76ea577ca410c42f6f382b76 |
| contracts/interfaces/IAegentPurchaseReceiptSource.sol | 28 | 52abd846c87734040bfb375177186bff6d8b56f 9b23ddbeeb8a7a4f4c3d5badb |
| contracts/interfaces/IAegentRedemptionEndpoint.sol | 13 | b78ac12e384e2c71bdf33eb44a899c417c30eb 4a9376fb28351d85c50bcf369d |
| contracts/interfaces/IAegentRegistryBound.sol | 8 | bf53c7606cbc5853a74710c9fa31dfd256a3128 3eedaf7ede01e213b0f12bc84 |
| contracts/interfaces/IAegentSaleProceedsVault.sol | 12 | eb1005d38941efc7dfd9e8c961eb5a4df10f9a4 3f630330495dd82b73854c974 |
| contracts/interfaces/IAggregatorV3.sol | 17 | 2dc0d69856b9cf3579d866c1da3bb9baff2fe50 5d9702001fcddc47e319a2b7e |

## REPRODUCIBILITY NOTE

Recompute every printed file digest from normalized bytes, preserve the displayed order and then compare the aggregate scope root. A single mismatch invalidates downstream compilation, test and triage associations until a new manifest is frozen. The register intentionally prints full SHA-256 values so analysis does not depend on a mutable repository reference.

| NORMALIZE | HASH | ORDER | BIND |
|---|---|---|---|
| Exact file bytes | Per-file SHA-256 | Canonical path list | Scope root + manifest |

# Conclusion

**RELEASE POSTURE: NO OPEN FINDINGS IN CURRENT REGISTER. LOCAL PASS COUNTS DO NOT CLOSE SHARED-CONTEXT BLOCKERS.**

Within the current source scope, the shared register records 9 tracked findings and the current closure summary is: All 9 tracked source-level findings are remediated and verified in the final frozen source. Production deployment, address/bytecode binding and continuing operations remain separate assurance gates.

The bound local evidence compiled 34 Solidity files, recorded 245 passing / 1 intentional exclusions on chain 56, recorded 1 passing / 0 excluded for the wrong-chain guard on chain 97, and found 0 known production npm advisories. Release posture remains NO OPEN FINDINGS IN CURRENT REGISTER: REGISTER: All 9 tracked source-level findings are remediated and verified in the final frozen source. Production deployment, address/bytecode binding and continuing operations remain separate assurance gates..

This conclusion is limited to the frozen source and local evidence identified in this report. Production deployment evidence and continuing operational controls remain separate assurance classes.

## DELIVERY AND RELEASE CHECKLIST

The deliverable package comprises the 42-page report, two-page executive summary, frozen source register, evidence manifest and local verification outputs. Reproduction starts by checking document and manifest hashes, restoring the recorded toolchain, compiling the frozen scope, running chain-56 and chain-97 suites, rerunning Solhint and verifying dependency-audit results. Release posture is NO OPEN FINDINGS IN CURRENT REGISTER for the current source register.

| DOCUMENTS | SOURCE PROOF | EXECUTION | FINDINGS |
|---|---|---|---|
| 42 + 2 pages | 11 hashes + root | Compile / tests / Solhint | 9 verified |

# Disclaimer

**END OF 42-PAGE AEGENT SECURITY ASSESSMENT**

CertiK conducted this point-in-time technical security assessment and issues the report for the exact AEGENT source scope, finding register and evidence identity printed herein. AEGENT is the assessed project and source-evidence provider.

This point-in-time assessment does not cover later source changes, compiler or dependency substitutions, proxy or address changes, external token implementation changes, oracle operator conduct, private-key custody, frontend compromise, market manipulation, legal compliance or economic performance. Mathematical formal verification was not part of the assessment methodology.

The report is not a warranty, guarantee, certification, investment recommendation or statement that the software is free from defects. Smart-contract systems involve technical, operational, governance and economic risks. Users and deployers remain responsible for independent due diligence, safe configuration and key management.

Only the files and hashes printed in this issue are within scope. Any modification, deployment change, external dependency change or configuration change requires fresh validation.

## SCOPE-BOUNDARY SUMMARY

Readers should preserve this document with its hashes and evidence run. Later code, configuration, deployment, market or dependency changes are separate assessment objects. CertiK issues this assessment for the exact frozen scope recorded here; deployment and continuing operational controls must be verified independently of the source snapshot.

| ISSUER | CLIENT | ASSESSMENT | DEPLOYMENT |
|---|---|---|---|
| CertiK | AEGENT | Point-in-time frozen source | Separate verification gate |