Falcon-512 Integration (Current)

Date: 2026-04-10

This document is the active Falcon-512 integration reference for Atho. It covers signing and verification flow, byte-policy enforcement, runtime binary controls, and operational checks required to keep cryptographic behavior deterministic across nodes.

- Runtime Model

Signing and verification are orchestrated through:

- Src/Accounts/falconcli.py

Consensus validation path references:

- Src/Transactions/txvalidation.py::_validate_signature
- KeyManager.verify_with_pubkey(...)
- FalconCLI.verify(...)

Runtime binary resolution prefers canonical pinned artifacts in Binaries/<platform-tag>/.

- Key and Signature Byte Policy

Current policy constants in Src/Utility/const.py:

- canonical Falcon public key size: 897 bytes (FALCON_PUBKEY_BYTES),
- legacy public key size compatibility: 1024 bytes (FALCON_PUBKEY_LEGACY_BYTES), disabled by default,
- compressed signature target: 666 bytes (FALCON_SIG_COMPRESSED_TARGET_BYTES),
- accepted signature window: 600..690 bytes (FALCON_SIG_MIN_BYTES..FALCON_SIG_MAX_BYTES).

Consensus checks enforce these bounds before invoking cryptographic verification.

- Encoding and Wire Behavior

Atho uses a binary-first tx transport (ATX2) with witness as raw bytes. API compatibility laye may expose witness fields using canonical text-safe encodings, but validation always decodes back to byte form and applies policy checks on bytes.

Practical implication:

- display format can vary by API surface,
- consensus acceptance rules remain byte-deterministic.
- Signing Flow

Standard signing pipeline:

- construct canonical no-witness signing body,
- hash signing body with SHA3-384,
- sign digest via Falcon CLI bridge,
- attach signature/public key witness fields.

Determinism requirements:

- canonical field ordering,
- stable serialization separators,
- explicit decimal/atom normalization before digesting.
- Verification Flow

Standard verification pipeline:

- strip witness fields and reconstruct canonical signing body,
- recompute SHA3-384 digest,
- decode witness signature/public key,
- enforce byte-length policy,
- run Falcon verification via configured verifier path.

Any mismatch in canonical body reconstruction invalidates the signature regardless of witness payload shape.
- Optional FFI Verification Path

An optional shared-library verifier can be enabled with explicit env configuration:
- ATHO_FALCON_FFI_ENABLE=1
- FALCON_VERIFY_SO=<absolute-path>
- FALCON_VERIFY_SO_SHA3_384=<expected-digest>

If FFI is unavailable or fails pin checks, runtime can fall back to CLI verification according to current policy flags.
- Binary Pinning and Integrity Controls

Integrity metadata locations:
- Binaries/pin_registry.json
- Binaries/<platform-tag>/binary_meta.json

Strict mode:

With strict mode enabled, unexpected binary paths or digest mismatches are rejected. This protects against accidental drift and malicious binary substitution.
- Operational Checklist

After Falcon-related changes:
- rebuild Falcon CLI/shared verifier artifacts,
- refresh pin metadata,
- run tx signing/verification smoke tests,
- run full unit/integration suite for tx validation paths,
- confirm explorer/API endpoints still decode witness fields correctly.

Command references:
- Migration and Compatibility Notes

Legacy pubkey acceptance (1024-byte) should remain disabled unless a deliberate migration wind is approved. Re-enabling compatibility broadens acceptance surface and should be time-bounded with explicit network coordination.

When compatibility mode is temporarily enabled:
- document activation height and deactivation plan,
- track acceptance counts,
- return to canonical-only mode as soon as migration completes.
- Policy Snapshot Context

Related production policy values (not Falcon-specific, but relevant to tx lifecycle):

- block target 120s, retarget interval 180,
- tx confirmations 10, private tx confirmations 10, coinbase maturity 150,
- fee floor 500 atoms/vB, min tx fee 200,000 atoms.

Falcon signatures protect transaction authenticity; these constants govern confirmation and economic policy around those authenticated transactions.
- Bottom Line

Falcon-512 integration in Atho is operationally mature when three things remain true:
- byte-level policy checks are enforced before verify,
- canonical signing-body reconstruction is deterministic,
- runtime verifier binaries are pin-validated from canonical paths.

Maintaining these guarantees keeps transaction signature behavior stable, auditable, and consensus-safe.