

KFIF ENTERPRISE

v5.1.0 Final Release Report

Kelibatmu Forensic Interchange Format platform

FINAL DECISION: GO

Release date: 12 August 2026

Distribution: proprietary, entitlement-gated evaluation

This report is the canonical post-signing release record for the exact v5.1.0 candidate. It does not alter the signed manifest or any immutable v5.0.0 evidence.

1. Executive decision

Decision	GO
Candidate	c5cc1377140174e0c9f9b2a6e6dbe515da0963fc
Product	KFIF Enterprise v5.1.0
Distribution	ENTITLEMENT_GATED
Critical/high blockers	None unresolved

The final candidate passed technical acceptance, was signed by the approved publisher identity, and independently verified with public-key-only verification as SIGNED_TRUSTED. The pre-signing readiness record remains immutable and correctly shows the owner signature as pending at the time it was included in the manifest. This post-signing report closes that gate.

2. Candidate and cryptographic identity

Object	Verified digest
Main archive SHA-256	b572f2e465da9638ef2ca51100fb7c818d70ac941c3367b5f33708c7ab44d10a
SBOM SHA-256	f2f066138e2ea4264ee90163648455dcb8af3c92b1c5d97611b8bad0ebffc258
Manifest SHA-256	538041ae4d4e20c994701920e86fb295fc92c13dd7910ba34143f250f2725171
Signature SHA-256	e3b721450d15713071d05012a5bc90cfd05dbe09359cbc6a8a6dd7c9bc013d43

Publisher signing

Algorithm: Ed25519

Purpose: release_signing

Key ID: kshield-release-2026-01

Public fingerprint SHA-256: d99fce706390efbd03d01839056cc4ff5705e5e7c94c650cab4b25b65e6f333f

Verification result: SIGNED_TRUSTED; all 12 manifest entries verified.

3. Acceptance evidence

Control	Result
Full unittest discovery	1,152 passed, 2 skipped, 0 failed
Focused licensing acceptance	28 passed, 0 failed
Public-site regression	56 passed, 0 failed
K-Shield Monitor regression	60 passed, 0 failed
Compileall	PASS
Fresh install and dependency check	PASS
SBOM and manifest integrity	PASS
Normalized source archive reproducibility	PASS - two archives, identical SHA-256
Private-key and secret scan	PASS
Production licensing public trust	PASS

4. Licensing security boundary

The exact evaluation period is 14 consecutive days. It begins only after the first successful v5.1.0 runtime initialization - not when an email is submitted, verified, entitled, linked, or downloaded. Runtime authorization is centralized and fails closed for proprietary execution while retaining status, activation, integrity verification, and appropriate read-only/export access. User data is never deleted, encrypted, or held hostage on expiry.

Runtime states

TRIAL_ACTIVE, TRIAL_EXPIRED, LICENSED, LICENSE_INVALID, LICENSE_EXPIRED

Production licensing trust

Domain: KFIF-ENTERPRISE-RUNTIME-LICENSE-V1

Purpose: licensing

Fingerprint SHA-256: feb70bf07b9b7278f2476bcd4b82c6d7665f68de334446276fb06de64ea4e944

Activation: offline Kelibatmu-signed Ed25519 license token; runtime contains public verification material only.

Security result

PASS for the implemented boundary: bounded parsing, device/product/domain/key validation, atomic and restrictive state persistence, clock rollback detection, failed-activation preservation, and no runtime network dependency. Production private licensing material was not used in acceptance fixtures and is absent from product artifacts and reports.

5. Evaluation distribution and privacy

The supported public flow is: email request, single-use verification email, automatic entitlement, second email with a single-use authorized download link, installation, then first successful runtime initialization. The download link is valid for exactly ten minutes. The main archive is held outside the public static tree; anonymous, expired, invalid, and replayed requests fail closed. Successful completed archive delivery is counted once; interrupted full delivery remains safely retryable and partial ranges do not inflate the count.

Privacy controls

Only the minimum required personal state is retained. Pending email is encrypted and removed after entitlement delivery; persisted tokens are hashes. Raw visitor IP is not retained for licensing or trial accounting. KPanel displays aggregate funnel metrics only. No marketing consent or telemetry requirement is implied.

Transactional mail

A dedicated KFIF-only Resend SMTP credential uses port 587 with STARTTLS required and sender noreply@kelibatmu.com. Isolated real-provider acceptance completed two request/verification sequences and four accepted messages. The existing Kelibatmu production mail credential remained separate and healthy.

6. Release operations and preservation

The v5.1.0 archive is deployed byte-for-byte from the signed candidate into a private release directory. Public verification metadata includes checksums, SBOM, manifest, detached signature, publisher public key, and this report; the main archive is not placed in that public directory. Scoped rollback archives are retained and readable before promotion.

v5.0.0 historical GA

KFIF Enterprise v5.0.0 remains a valid immutable signed historical GA release. Its anonymous main-archive distribution remains withdrawn because that runtime predates trial enforcement. Historical evidence, checksum, manifest, signature, public key, SBOM, release notes, and final report remain preserved. The release is not described as revoked, compromised, or invalid.

7. Known limitations

SMTP evidence proves application-to-provider acceptance but not independent mailbox placement or message opening because the scoped SMTP credential cannot query provider sent-status APIs. The offline licensing state does not claim resistance to privileged filesystem rollback, full machine or VM snapshot restoration, replacement of runtime/trust code, or complete machine restoration. Reproducibility applies to the normalized source archive, not a platform binary build.

Final disposition

GO - KFIF Enterprise v5.1.0 is approved for scoped production publication using entitlement-gated evaluation distribution.