fips-pad

Security Posture Statement (SPS)

Document version: 0.1-draft   Date: 2026-02-02

Purpose

This document describes the security posture, cryptographic dependencies, and operational assumptions of fips-pad, a deliberately minimal offline encrypted notepad application. It is intended to be readable by engineers and security reviewers. It is **not** a certification, attestation, or audit report.

Non-claims (read carefully)

- fips-pad is **not** a FIPS 140-3 validated cryptographic module.

- fips-pad does **not** claim compliance with NIST SP 800-53 as an assessed information system.

- fips-pad does **not** provide enterprise identity, centralized audit pipelines, incident response, or continuous monitoring.

System overview

Scope	Single-user, offline desktop application. Local encrypted files only.
Data handled	User-supplied note text. No telemetry. No network calls. No cloud sync.
Primary security goals	Confidentiality at rest; tamper detection for stored files; minimal attack surface; fail-closed behavior.
Threats considered	Lost/stolen device; opportunistic local file access; offline file tampering.
Threats out of scope	Compromised OS/kernel; runtime memory compromise; keyloggers; hostile admin; multi-user access control.

FIPS posture and runtime gating

fips-pad is designed to operate only when a platform-appropriate FIPS-approved cryptographic surface is available and verified by a strict gate. The gate is fail-closed: if the gate cannot be verified, the application refuses to run.

Platform	Backend used	Gate condition (strict)	User experience when failing
Windows 10/11	Windows CNG / BCrypt APIs	OS reports FIPS compliance enabled via **BCryptGetFipsAlgorithmMode()**.	Refuse to run; guide user to enable the Windows FIPS policy and reboot.

macOS	Apple system crypto (CommonCrypto / Security framework)	OS major version + architecture must be allowlisted based on Apple's published macOS security certifications for FIPS 140-3 user-space modules. App also constrains itself to approved algorithms/modes and runs a small OS-crypto self-test.	Refuse to run on macOS versions not listed as certified (e.g., in review / review pending).
Linux (optional)	OpenSSL configured for FIPS provider (distro dependent)	FIPS-enabled OS configuration is detected; otherwise fail.	Refuse to run; point to canonical FIPS-enabled distro examples.

Development bypass

Development builds may include a temporary **--skip-check** flag that bypasses the FIPS gate. This flag is intended solely for development and testing on non-allowlisted systems and is removed from production releases.

Cryptographic design (high level)

• All protected note files are stored as authenticated ciphertext (AEAD).

• Keys are derived from a user passphrase using an approved KDF (platform backend dependent).

• Nonces/salts are generated using OS RNG.

• Atomic encrypted writes are used (write temp, fsync, rename) to avoid partial-file corruption.

• The application does not intentionally write plaintext note content to disk (including temp files).

NIST SP 800-53 control selection (subset)

fips-pad uses NIST SP 800-53 Rev. 5 as a control vocabulary to select and tailor a small subset of controls that are appropriate to a single-user offline application. This is documentation discipline, not a compliance claim.

Control	Status	How fips-pad addresses it (scoped)
SC-13 (Cryptographic Protection)	Implemented	All crypto uses OS backends; strict gate requires FIPS-approved mode/surface.
SC-28 (Protection of Information at Rest)	Implemented	Notes stored only as authenticated ciphertext; no plaintext file format.
SI-7 (Integrity)	Implemented	AEAD authentication failure treated as tamper/corruption; fail closed.
CM-7 (Least Functionality)	Implemented	No network stack; no plugins; no scripting; minimal UI surface.
AU-2 (Event Logging)	Implemented (minimal)	Local-only security events (gate failures, decrypt/auth failures), no content logging.
AC / IA families	Not applicable	Single-user offline tool; no shared authorization boundary.
CA / IR / PL / PM / RA / SR families	Out of scope	No organizational program claims; not an assessed system.

Supported platforms (strict gate)

The strict macOS allowlist is derived from Apple’s published macOS security certifications page for FIPS 140-3. At the time of writing, Apple lists macOS 11 (Big Sur), macOS 12 (Monterey), and macOS 13 (Ventura) with certified user-space software modules. Newer releases may appear as 'in review' or 'review pending' and are rejected.

Reviewer checklist (what to verify)

• Run `fips-pad --check` to see platform gate status and backend.

• Verify Windows reports FIPS mode enabled prior to use (BCryptGetFipsAlgorithmMode).

• Verify macOS version/arch is allowlisted and that only OS crypto APIs are linked.

• Confirm app contains no networking (no sockets) and no telemetry endpoints.

• Confirm file format stores ciphertext only; authentication failure yields a single generic error.

Signature

Prepared by: ________________________________ Date: ____________________
Role/Organization: __________________________

This document describes intended behavior for the referenced version. It does not constitute certification or legal attestation.

References

• Apple Platform Certifications - macOS security certifications (FIPS 140-3 tables). Apple Support.

• Apple: Security certifications for Apple Applications (notes on CMVP certificates and per-major-release validation).

• Microsoft Docs: BCryptGetFipsAlgorithmMode (determines whether FIPS compliance is enabled).

• Microsoft Docs: 'System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing' policy setting.