RETSU - ERASURE

NIST SP 800-88 REV. 2 CONFORMANCE STATEMENT

Product: Retsu - Erasure
Vendor: Dehhani Ltd
Applicable from version: 2.2.4
Document Version: 1.4
Document Date: 2026-07-28
Author: Ibrahim Dehhani, Founder, Dehhani Ltd

1. PURPOSE

This document is a vendor self-attestation that the data sanitization functions implemented in Retsu - Erasure conform to the methods, sanitization-assurance requirements, and cryptographic-erase guidance defined in NIST Special Publication 800-88 Revision 2, Guidelines for Media Sanitization (Chandramouli & Hibbard, NIST, September 2025), which supersedes Revision 1 (December 2014).

Retsu - Erasure operates as a standalone Linux-based live-boot environment, independent of any operating system installed on the target device. This ensures that the sanitization process cannot be intercepted, modified, or undermined by software or malware residing on the target drive.

This is a vendor statement, not a third-party certification. NIST does not issue product certifications for SP 800-88 conformance; no such program exists. Customers requiring independent validation are referred to a third-party security testing laboratory's assessment report and/or to the ADISA Asset Recovery Standard certification.

2. SCOPE AND SUPPORTED MEDIA

This statement covers Retsu - Erasure v2.2.4 and all subsequent versions unless superseded by a later revision of this document.

Supported Media:

- **SATA Hard Disk Drive (HDD)**
  Clear: Yes
  Purge: Yes (ATA Secure Erase)
  Notes: Full overwrite and hardware erase supported
- **SATA Solid State Drive (SSD)**
  Clear: Yes (with warning)
  Purge: No — fail-closed in this release. ATA Secure/Enhanced Erase is enabled only for media positively identified as rotational; on solid-state or unknown-rotation SATA media, NIST Purge refuses to run with the diagnostic that flash media require model/firmware-specific coverage evidence, rather than issuing an erase whose flash-level coverage cannot be evidenced.
  Notes: Operator warned that software overwrite cannot reach wear-levelled blocks. Sanitization of SATA SSDs is limited to NIST Clear (with warning) in this release.

- **NVMe Solid State Drive (SSD)**
  Clear: Yes (with warning)
  Purge: Yes (NVMe Sanitize Block Erase; NVMe Sanitize Overwrite). NVMe Sanitize Cryptographic Erase and NVMe Format Cryptographic Erase are implemented but administratively disabled fail-closed in this release, pending model/firmware-specific cryptographic-erase evidence — see §4.4.
  Notes: Operator warned that software overwrite cannot reach wear-levelled blocks; Purge recommended
- **USB flash drives**
  Not supported — not a target platform for Retsu - Erasure
- **eMMC / embedded storage**
  Not supported — not a target platform for Retsu - Erasure

Sanitization Methods in the Retsu - Erasure Operator Interface:

- NIST Clear (SP 800-88 Rev. 2) — maps to SP 800-88r2 Clear (§3.1.1)
- NIST Purge (SP 800-88 Rev. 2) — maps to SP 800-88r2 Purge (§3.1.2), automatic best method

Legacy Methods (provided for policy compatibility only — not claimed as SP 800-88r2 conformant):

- HMG IS5 Baseline (1-pass)
- HMG IS5 Enhanced (3-pass)
- DoD 5220.22-M (3-pass)
- DoD 5220.22-M (7-pass)
- Gutmann (35-pass)
- Zero Fill (1-pass)

Note on legacy methods: SP 800-88r2 §3.1.1 explicitly characterizes the multi-pass DoD 5220.22-M approach as obsolete and notes that, for solid-state media, multi-pass overwrite "should be avoided as very little confidentiality protection is achieved." Retsu - Erasure surfaces a warning to the operator on solid-state media when any software-overwrite method is selected. The HMG IS5 Baseline and Zero Fill methods are implemented identically to the NIST Clear technique — a single 0x00 overwrite pass with the same zero-content verification — but are reported under their own method labels and carry no NIST standard claim on the resulting evidence report.

3. REFERENCE STANDARD

NIST Special Publication 800-88 Revision 2
Guidelines for Media Sanitization
Ramaswamy Chandramouli and Eric A. Hibbard, September 2025
DOI: https://doi.org/10.6028/NIST.SP.800-88r2
Page: https://csrc.nist.gov/pubs/sp/800/88/r2/final

This document maps Retsu - Erasure's implementation against the following sections of SP 800-88r2:

- §3.1 — Sanitization Methods (Clear, Purge, Destroy)
- §3.1.1 — Clear Sanitization Method
- §3.1.2 — Purge Sanitization Method

- §3.2 — Use of Cryptography and Cryptographic Erase
- §3.2.3 — Sanitization of Keys
- §4.5 — Sanitization Assurance (§4.5.1 Verification, §4.5.2 Validation)
- §4.6 — Documentation
- Appendix C — Sample "Certificate of Sanitization" Form

Relationship to IEEE 2883: SP 800-88r2 explicitly delegates technology-specific sanitization technique guidance to IEEE 2883 — IEEE Standard for Sanitizing Storage and IEEE 2883.1. Where this document refers to ATA Secure Erase, NVMe Sanitize, and NVMe Format Cryptographic Erase, it refers to the technique definitions established in those standards. This document does not claim independent conformance to IEEE 2883; it claims that Retsu - Erasure implements the technique families that IEEE 2883 catalogues and that SP 800-88r2 §3.1.2 accepts as Purge.

4. METHOD-BY-METHOD CONFORMANCE

4.1 NIST Clear

SP 800-88r2 §3.1.1 definition: *"A method of sanitization that applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple, non-invasive data recovery techniques using the same interface that is available to the user."*

Retsu - Erasure implementation:

Retsu - Erasure's Clear sanitization module performs a single-pass overwrite of every host-addressable logical block on the target device with all-zero data, issued as standard host logical-block writes at the block-device level in one sequential pass. On ATA drives, sanitization is preceded by mandatory hidden-area exposure: Host Protected Area and Device Configuration Overlay configurations are detected and permanently removed, with post-checks proving the full native capacity is host-visible, before the overwrite begins — so coverage extends to the full native capacity, and the job is refused if hidden-area coverage cannot be proven. Post-overwrite zero-content verification (§5.1) is a hard gate: any sampled non-zero byte, or any unreadable sampled region, fails the job.

SP 800-88r2 §3.1.1 explicitly clarifies that multi-pass overwrite is not required and that the obsolete DoD 5220.22-M multi-pass requirements have been superseded.

Limitations explicitly acknowledged in SP 800-88r2 §3.1.1: Software overwrite using read/write commands "make[s] it infeasible for a user to sanitize all previous data using this approach because the device cannot support directly addressing all areas in which sensitive data has been stored using the native read and write interface." This applies to flash-memory devices with spare cells and wear levelling. Retsu - Erasure detects solid-state media automatically and surfaces a warning to the operator recommending NIST Purge for SSDs, in compliance with this guidance.

4.2 NIST Purge — NVMe SSDs

SP 800-88r2 §3.1.2 definition: *"A method of sanitization that applies physical or logical techniques to render target data recovery infeasible using state-of-the-art laboratory techniques."*

Retsu - Erasure implementation:

Retsu - Erasure reads the controller's Identify Controller data — Sanitize Capabilities (SANICAP), Optional Admin Command Support (OACS), and Format NVM Attributes (FNA) — and attempts the following techniques in priority

order. A technique is skipped when its capability is not reported, or when required eligibility evidence is not established; the next technique is attempted when a command or its completion evidence fails. Each technique attempted is one of those catalogued by IEEE 2883 as a Purge sanitization technique for NVMe storage and is recognised by SP 800-88r2 §3.1.2 as a logical Purge technique.

1. NVMe Sanitize — Block Erase (SANACT=2)

Aligned with the NVM Express Base Specification Sanitize command, Block Erase action. Instructs the controller to perform a media-level erase of all user data in the NVM subsystem. SP 800-88r2 §3.1.2 explicitly lists "block erase" among the acceptable logical Purge techniques. Gated on the SANICAP Block Erase capability bit.

2. NVMe Sanitize — Cryptographic Erase (SANACT=4)

Implemented, but administratively disabled fail-closed in this release: the technique is skipped, with the recorded rationale that command capability and completion do not establish the model/firmware-specific cryptographic prerequisites required to claim Cryptographic Erase as Purge (see §4.4). The command is not issued while eligibility is not established.

3. NVMe Sanitize — Overwrite (SANACT=3, OWPASS=1, OVRPAT=0x00000000)

Aligned with the NVM Express Base Specification Sanitize command, Overwrite action. Instructs the controller to perform one controller-managed overwrite pass with an all-zero pattern across the NVM subsystem, including regions not reachable through host logical-block writes. Gated on the SANICAP Overwrite capability bit.

4. NVMe Format — Cryptographic Erase (SES=2)

Implemented, but administratively disabled fail-closed under the same cryptographic-erase eligibility gate as technique 2 (see §4.4). When eligible, its scope is derived from FNA: a single subsystem-wide command where FNA proves cryptographic erase applies to all namespaces; otherwise one command per enumerated namespace — and any ambiguity in Format capability, cryptographic-erase scope, or namespace enumeration fails closed rather than guessing. Secure Erase Setting 1 (User Data Erase) is not claimed as Purge by Retsu - Erasure, because it permits an FTL-only reset that does not satisfy SP 800-88r2 Purge requirements.

Command submission alone is never treated as completion. A Sanitize operation is accepted only on controller completion evidence read from the Sanitize Status Log (log page 0x81): SSTAT must report successful completion, the logged sanitize action and command dword (SCDW10) must exactly match the submitted command, the command must have been accepted by the controller, and fresh-run linkage must prove the terminal log belongs to this operation. Ordinarily the Global Data Erased attribute must also be set; a controller that reports successful completion without setting Global Data Erased is accepted only as a recorded controller anomaly — the completion is marked "completed with controller anomaly" and requires proof that the per-run 4 KiB challenge marker was destroyed, with the anomaly and its proof preserved on the evidence report — established by a per-run 4 KiB random challenge written at the device midpoint before the command (whose SHA-256 digest must no longer be readable back unchanged afterwards), by an observed in-progress status during polling, or by an observed status transition from the pre-command baseline log. A terminal log that remains indistinguishable from the pre-command record beyond a 30-second grace window fails the erase. A Sanitize Progress value of FFFFh is treated as not-applicable, never as a measured 100%.

In addition, a pre/post block comparison — SHA-256 of 4 KiB blocks at five fixed reference points (first block, 25%, 50%, 75%, last block) — is recorded as supplementary, non-authoritative evidence. An unchanged comparison is not treated as a sanitize failure, because a compliant controller may legitimately return deallocated or unchanged-reading blocks after sanitize; the command and status-log evidence remain authoritative.

Retsu - Erasure does not silently downgrade Purge to Clear — if all hardware Purge methods fail or are unsupported, the job fails with a clear diagnostic and the operator is instructed to use NIST Clear instead.

The exact technique that succeeded is recorded on the sanitization evidence report (e.g., "NVMe Sanitize Block Erase (SANACT=2)"), together with the exact command line, opcode and command dword, submission and acceptance timestamps, exit status, bounded command output, and the controller's completion evidence. The report itself asserts no final standard claim; the standard determination is made at organizational validation (§5.2).

4.3 NIST Purge — SATA HDDs

Retsu - Erasure implementation:

Retsu - Erasure issues standard ATA Security feature-set commands to perform hardware-level erasure on SATA drives positively identified as rotational (HDDs). Solid-state and unknown-rotation SATA media are refused for ATA Secure Erase, fail-closed (see §2). Before any ATA sanitization, the storage interface itself must be positively established — by transport reporting or by a successful ATA IDENTIFY (USB-attached bridges are probed rather than assumed, since a USB bridge may front an ATA device); if the interface cannot be established as ATA or as a proven non-ATA protocol, whole-device erasure is refused because HPA/DCO applicability would be unknown.

1. Detect frozen state

Retsu - Erasure checks the drive's ATA Security feature-set status via ATA IDENTIFY. If the drive reports "frozen" (a common state after BIOS initialisation), Retsu - Erasure initiates an ACPI S3 suspend cycle to clear the frozen state; system resume depends on the platform's wake behaviour. After the cycle the security state is probed again, and unless ATA IDENTIFY positively proves that Security Erase is supported and the drive is not frozen — an unknown or unprovable state is treated the same as frozen — the operation fails with a clear diagnostic instructing the operator to reconnect the drive or use NIST Clear.

2. Dual capability probe

The ATA Security capability probe is performed twice: once as a preflight before hidden-area exposure, and again at the command boundary immediately before the erase. If the reported support or mode bits differ between the two probes, the erase is refused. Every probe — including failed ones — is recorded as capability-check evidence on the report.

3. Hidden-area exposure (HPA/DCO)

Before any ATA sanitization — Purge or Clear — Retsu - Erasure detects Host Protected Area and Device Configuration Overlay configurations (ATA READ NATIVE MAX and DCO IDENTIFY interrogation) and permanently removes them (persistent SET MAX ADDRESS; DCO restore), including re-exposing any HPA revealed by the DCO restore. Post-checks must prove that the full native capacity is host-visible; each capacity change is recorded as evidence with drive-identity continuity checks, and prior HPA/DCO configuration is deliberately not reinstated on decommissioned media. If hidden-area coverage cannot be proven, the job is refused before any erase command is issued, and hidden-area coverage independently gates the final technical assessment.

4. Set temporary user password

A temporary ATA security password is set on the drive to enable the Secure Erase command set. The password value is redacted from all recorded command evidence.

5. Issue Enhanced Secure Erase (preferred)

ATA Enhanced Secure Erase (per ATA-8/ACS-4, Security Erase Unit Ext) instructs the drive's firmware to erase all user data including reallocated sectors. This is one of the techniques catalogued by IEEE 2883 as a Purge sanitization technique for SATA drives and is accepted by SP 800-88r2 §3.1.2 as a logical Purge technique.

6. Fallback to Standard Secure Erase

If Enhanced Secure Erase is not supported by the drive, Retsu - Erasure falls back to Standard ATA Secure Erase, which still qualifies as Purge for HDDs.

7. Cleanup

If the operation fails before the ERASE UNIT command has been submitted, Retsu - Erasure disables the temporary password so the drive is left in a non-locked state. Once the erase command has been submitted, or when the failure is a target-safety abort (the drive's identity or the lifecycle lock could not be re-proven), no further commands are issued to the drive — the temporary password is deliberately left in place rather than acting on a device in an indeterminate or unproven state, and the condition is recorded on the evidence report. The temporary password value is fixed and documented internally, so an affected drive remains recoverable by the operator.

The exact technique used is recorded on the sanitization evidence report (e.g., "ATA Enhanced Secure Erase"), together with the exact command evidence. The report asserts no final standard claim; the standard determination is made at organizational validation (§5.2).

4.4 Cryptographic Erase

SP 800-88r2 §3.2: *"[CE is] a purge sanitization technique known as cryptographic erase (CE). At a basic level, CE is based on the sanitization of keys used to encrypt data or to prevent access to the keys that encrypt data."*

SP 800-88r2 §3.2.3 lists four categories of valid target cryptographic keys: symmetric data-encryption keys, symmetric key-wrapping keys, symmetric master/key-derivation keys, and private key-transport keys.

Retsu - Erasure implementation:

Retsu - Erasure implements the NVMe Cryptographic Erase command paths — Sanitize Cryptographic Erase (SANACT=4) and Format NVM with Secure Erase Setting 2 — but currently declines to execute them, fail-closed. SP 800-88r2 §3.2.4 makes CE assurance depend on evidence about the drive's cryptographic implementation that a host-issued interface command cannot itself establish. Retsu - Erasure therefore records CE Purge eligibility as "not established" unless model/firmware-specific evidence has been recorded covering, at minimum:

- applicable FIPS 140 validation and approved cryptographic implementation and use;
- proof that the target data was never stored in plaintext and was protected by keys of adequate strength and entropy;
- proof that the command permanently zeroizes every target key and all relevant key-hierarchy copies;
- proof that no injected, escrowed, or externally retained key can recover the target data; and
- vendor-documented behaviour for the exact drive model and firmware revision.

When a Cryptographic Erase technique is reached in the Purge priority order without that evidence, the technique is skipped and the recorded rationale states why; sanitization proceeds to a non-CE technique or the job fails without downgrade. Capability support (SANICAP, OACS, FNA) is still interrogated and recorded first, and command completion alone is never treated as establishing the cryptographic prerequisites: even a completed CE command would not be accepted as Purge without the recorded eligibility evidence. Retsu - Erasure does not perform software-side cryptographic erase, and has no ATA SED cryptographic-erase mode — ATA Enhanced Secure Erase is reported as Enhanced Secure Erase and is never claimed as Cryptographic Erase.

§3.2 pre-condition (no plaintext prior to CE) and §3.2.4 implementation-quality guidance are addressed by the same evidence gate: rather than relying on the SED's own conformance implicitly, Retsu - Erasure withholds the CE Purge claim until the §3.2.4-relevant assurances above are recorded for the exact model and firmware. Customers requiring

CE-based sanitization should obtain those assurances from the drive vendor (e.g., FIPS 140-2/-3 validation records, TCG Opal conformance) — Retsu - Erasure does not perform cryptographic implementation testing of the target drive.

5. SANITIZATION ASSURANCE

SP 800-88r2 §4.5 introduces Sanitization Assurance, which combines two distinct activities:

- §4.5.1 Sanitization Verification — inspecting the outcome of the sanitization technique to determine whether it completed successfully (e.g., did the command return success, were there errors).
- §4.5.2 Sanitization Validation — deciding whether the target data was effectively sanitized to a level acceptable to the organisation.

5.1 SANITIZATION VERIFICATION (§4.5.1)

Retsu - Erasure performs technique-completion inspection and block-sample inspection after every erase operation:

Software overwrite (NIST Clear, HMG IS5 Baseline, Zero Fill, DoD 5220.22-M variants — every method ending in a 0x00 pass):

Read 10 regions of 4 KiB: the first region and the final region are always sampled, and the remaining eight are selected pseudorandomly across the reported logical capacity. Every byte of every sampled region must equal 0x00. Any non-zero byte — or any unreadable sampled region — constitutes a verification failure, and any verification failure fails the job. Methods that end on a non-zero pass (Gutmann; HMG IS5 Enhanced) receive readability sampling of the same regions instead of a zero-content check. Each sampled location and its outcome is recorded on the evidence report.

Hardware Purge:

(a) Authoritative completion evidence (NVMe Sanitize): acceptance is decided from the controller's Sanitize Status Log as described in §4.2 — successful SSTAT, sanitize-action and SCDW10 match, command acceptance, fresh-run linkage (per-run 4 KiB challenge, observed in-progress status, or observed status transition), and Global Data Erased — or, failing GDE, a recorded controller anomaly backed by destruction of the per-run challenge marker. For ATA Secure Erase, acceptance is decided from command completion together with the capability, identity, and hidden-area evidence of §4.3.

(b) Supplementary pre/post comparison (NVMe techniques): SHA-256 of 4 KiB blocks at five fixed reference points (first block, 25%, 50%, 75%, last block) captured before and after the operation. A change in one or more reference blocks — or a device that already reads as predominantly zero — is recorded as supportive evidence. The comparison is explicitly recorded as supplementary and non-authoritative: an unchanged comparison does not fail a controller-verified erase, because a compliant controller may return deallocated or unchanged-reading blocks after sanitize.

(c) Supplementary post-erase read sampling at 10 regions of 4 KiB (first region, final region, remainder pseudorandom): for NVMe Sanitize/Format, unreadable or deallocated regions are tolerated as compliant post-sanitize behaviour; for ATA Secure Erase, every sampled region must be readable. Sampled locations and outcomes are recorded on the evidence report.

(d) For ATA drives, hidden-area coverage (§4.3) — and for any cryptographic-erase outcome, CE Purge eligibility (§4.4) — additionally gate the technical assessment.

Note: SP 800-88r2 §4.5.1 explicitly states that "elaborate sampling of an ISM's contents (e.g., full or representative) after clear or purge sanitization techniques is not necessary" unless required by organizational policy. Retsu - Erasure's

read sampling is supplementary to command/status completion evidence and exceeds the SP 800-88r2 minimum as an additional defensive measure.

5.2 Sanitization Validation (§4.5.2)

Retsu - Erasure separates the two §4.5 activities explicitly.

Locally, it produces an automated technical assessment of sanitization verification: a job passes only when the selected technique completed, read-sampling verification passed, controller completion evidence was accepted (NVMe), cryptographic-erase Purge eligibility was established for any CE outcome, and hidden-area coverage was proven for ATA media. The assessment, its rationale, and every underlying evidence record are written to the sanitization evidence report. Failures are surfaced to the operator with diagnostics.

The §4.5.2 validation decision — organizational judgment covering policy and method eligibility, data classification and confidentiality risk, scope and anomaly review, residual-risk acceptance, media disposition, and validator identity and authority — is deliberately not made locally. The evidence report deliberately records no local validation decision at all: it carries only the automated technical assessment (decision and rationale) and withholds any standard claim. Organizational validation status exists solely as a Portal record. Retsu - Portal records the formal validation and issues the final Certificate of Sanitization only after an authorized validator approves; the certificate carries the approved standard claim and links to the digest of the evidence it validates.

Retsu - Erasure does not silently downgrade a failed Purge to a successful Clear — if all hardware Purge methods are exhausted, the job is failed and the operator is instructed to select NIST Clear if they wish to proceed.

6. OPERATOR DECISION SUPPORT

Retsu - Erasure surfaces the following SP 800-88r2-aligned guidance to the operator at the point of erasure:

- **SSD warning (§3.1.1):** When the operator selects any software-overwrite method on a drive identified as solid-state, Retsu - Erasure warns: "This drive is solid-state. Software overwrite may not sanitise data in wear-levelled blocks or overprovisioned cells — per NIST SP 800-88 Rev. 2 §3.1.1, multi-pass patterns (DoD, Gutmann) provide little additional benefit on SSDs. NIST Purge (hardware erase) is recommended." When the rotation state cannot be determined, a corresponding caution is shown instead.
- **Frozen drive guidance:** If an ATA drive's security feature set is frozen and cannot be unfrozen, Retsu - Erasure fails the job with the diagnostic "Drive security is frozen and could not be safely unfrozen; reconnect the drive or use NIST Clear."
- **Hard fail on Purge unavailability:** If all hardware Purge methods fail or are unavailable, Retsu - Erasure does not silently fall back to a software overwrite; it fails the job with the diagnostic "NIST Purge failed — this drive does not support or rejected all hardware erase commands. Use NIST Clear (software overwrite) instead," including the per-technique detail, so the operator can make an informed decision. The same fail-closed posture applies up front: NIST Purge is refused on SATA media not positively identified as rotational (§2), and whole-device erasure is refused when the storage interface cannot be positively established (§4.3).

7. SANITIZATION EVIDENCE REPORT AND CERTIFICATE (§4.6, APPENDIX C)

For every terminal sanitization attempt — completed, failed, or stopped — Retsu - Erasure generates a sanitization evidence report (schema v2). The evidence report intentionally asserts no final standard claim and is not itself the

Certificate of Sanitization: the certificate contemplated by SP 800-88r2 §4.6 and Appendix C is issued by Retsu - Portal after formal organizational validation (§5.2), carries its own identifier and issue time, and links to the digest of the evidence report it validates. The evidence report records the fields below (Appendix C coverage plus controller-level evidence):

- **Make and model** — Drive manufacturer and model as reported by the device
- **Serial number** — Drive serial number
- **WWN and firmware revision** — Drive world-wide name and firmware revision
- **Media type** — Detected media type and transport (HDD / SATA SSD / NVMe SSD)
- **Sanitization method** — The selected erasure method, mapped to the NIST category (Clear / Purge); the requested standard is recorded separately from the final standard claim, which is withheld for validation
- **Sanitization technique** — The specific ATA or NVMe technique that was applied
- **Controller capabilities** — Raw and decoded SANICAP, OACS, and FNA evidence (NVMe); ATA Security capability probes (preflight and command-boundary)
- **Exact command evidence** — Full command line and argv, opcode and command dword, submission/acceptance timestamps and durations, exit status, and bounded command output for every attempt (append-only attempt history)
- **Controller completion evidence** — SSTAT, Global Data Erased (or a recorded, marker-backed controller anomaly), sanitize-action and SCDW10 match, and fresh-run linkage basis (NVMe)
- **Scope evidence** — Namespace enumeration and derived sanitize/format scope (NVMe); hidden-area assessment and capacity adjustments (ATA); media-interface assessment; drive-identity revalidations at command boundaries
- **Tool used, including version** — Retsu - Erasure application and OS image versions; for NVMe operations, the nvme-cli version is additionally recorded on the capability evidence and on each command record
- **Verification method** — Post-overwrite logical block content sampling (zero-final software methods) or post-hardware-command supplementary logical interface sampling with controller completion evidence (hardware Purge), as detailed in §5.1
- **Verification result** — Pass/fail status, sample count, sampled locations and outcomes, failure notes
- **Assessment status —** The automated technical assessment decision with rationale; organizational validation status is recorded by Retsu - Portal, not on the local evidence report
- **Date/time** — Start and end timestamps; sanitization duration recorded separately from total lifecycle duration (which includes evidence writing)
- **Person performing sanitization** — Operator/technician identification (when configured)
- **System specifications** — Host device model, system serial, CPU, installed memory, and BIOS version of the machine on which the sanitization was performed (recorded for audit context; not required by Appendix C)
- **Report identity and digest** — Report identifier and the SHA-256 digest of the on-media evidence JSON
- **Signature** — The validator attestation belongs to the Portal-issued Certificate of Sanitization; local evidence artifacts identify the operator/technician and carry a SHA-256 digest of the evidence rather than a signature line

Evidence reports are produced as machine-readable JSON with a human-readable HTML rendering. They are:

- Persisted locally to the device's erasure-reports store for immediate access.
- Submitted to Retsu - Portal (https://portal.retsu.uk) for centralised audit storage, formal organizational validation, and certificate issuance.
- Written to the sanitized drive itself (when supported): a small EFI System Partition labelled RETSU-WIPED carries sanitization-evidence-report.json and .html together with a bootable evidence presentation — powering on the wiped drive displays the branded evidence screen with menu actions (View Full Report — which redisplays the full graphical report, with a compact text rendering as fail-safe — Firmware Setup, Restart, Shut Down). The SHA-256 digest of the exact on-media JSON is displayed on that screen, embedded in its QR payload, and recorded in the on-media README, so the evidence travelling with the device can be verified in place (sha256sum sanitization-evidence-report.json). All on-media wording identifies the artifact as a sanitization evidence report, not a certificate.

8. WHAT THIS STATEMENT DOES NOT CLAIM

To be unambiguous about scope:

1. This is a vendor self-attestation, not a third-party certification or government accreditation. NIST does not issue certifications for SP 800-88r2 conformance; no vendor in the data sanitization space holds a "NIST certification" because none exists.
2. Retsu - Erasure does not implement Destroy (the third SP 800-88r2 sanitization method, e.g. shredding, incineration, melting, pulverising, disintegrating). Destroy is a physical-destruction process and is out of scope for any software product.
3. Retsu - Erasure's claimed conformance applies only to drives that respond truthfully to standard ATA/NVMe interrogation commands. A drive whose firmware misreports its capabilities or silently ignores sanitize commands cannot be detected by any software-based tool. SP 800-88r2 §3.1.2 acknowledges this: "such commands... require trust and assurance from the ISM vendor that the commands have been implemented as expected."
4. Software overwrite methods (NIST Clear) cannot reach blocks remapped or retired by SSD wear-levelling logic. SP 800-88r2 §3.1.1 explicitly acknowledges this; Retsu - Erasure surfaces it to the operator and recommends NIST Purge for SSDs.
5. Retsu - Erasure's HMG IS5, DoD 5220.22-M, and Gutmann methods are provided for policy compatibility only. They are not, and are not represented as, SP 800-88r2 Clear or Purge methods unless specifically equivalent (single-pass zero overwrite with verification). SP 800-88r2 §3.1.1 explicitly notes that the historical DoD 5220.22-M multi-pass requirements are obsolete and that for SSDs they "should be avoided."
6. Retsu - Erasure does not perform cryptographic implementation testing of Self-Encrypting Drives. As recommended by SP 800-88r2 §3.2.4, SED users should obtain cryptographic implementation assurance directly from the drive vendor (e.g., via FIPS 140-2/-3 validation reports or TCG Opal certifications).
7. Retsu - Erasure does not address partial ISM sanitization (SP 800-88r2 §4.2). All Retsu - Erasure methods sanitize the entire host-addressable area of the drive.
8. The NVMe Cryptographic Erase techniques (Sanitize SANACT=4; Format SES=2) are implemented but administratively disabled, fail-closed, in this release pending model/firmware-specific cryptographic evidence (§4.4). No Cryptographic Erase result is claimed as Purge, and no ATA cryptographic-erase mode exists.

9. ATA Secure/Enhanced Erase is offered only for SATA media positively identified as rotational. NIST Purge on SATA solid-state media is refused, fail-closed, rather than claimed (§2, §4.3).

9. DOCUMENT CONTROL

- **Document ID:** Retsu-NIST-800-88-CONF-001
- **Standard version:** NIST SP 800-88 Revision 2 (September 2025)
- **Applicable from:** Retsu - Erasure v2.2.4
- **Document version:** 1.4
- **Last reviewed:** 2026-07-28
- **Review cycle:** Annually, or upon any material change to the erasure subsystem, or upon publication of a new SP 800-88 revision or IEEE 2883 update
- **Authorized signatory:** Ibrahim Dehhani, Founder, Dehhani Ltd

REVISION HISTORY

Version 1.0 — 2026-04-08
Initial release, referencing NIST SP 800-88 Rev. 1 (December 2014).

Version 1.1 — 2026-04-08
Updated to reference NIST SP 800-88 Rev. 2 (Final, September 2025). Section references renumbered. Sanitization Assurance split into Verification and Validation per Rev. 2. Cryptographic Erase mapping aligned to Rev. 2 §3.2.3 key categories. Acknowledged IEEE 2883 delegation. Strengthened legacy-method language per Rev. 2's obsoleting of DoD 5220.22-M.

Version 1.2 — 2026-04-10
Removed internal code references. Added supported-media summary table. Added live-boot environment description. Added Retsu - Portal certificate submission to Section 7. Added revision history table. Branded as Retsu - Erasure / Dehhani Ltd. Changed version field to "Applicable from" model.

Version 1.3 — 2026-06-24
Rebranded all product references from "DSU" to "Retsu" throughout the document to reflect the product's renaming. Updated the product name in the document title, body, document-control fields, and footer accordingly; the Document ID (RETSU-NIST-800-88-CONF-001) and all NIST SP 800-88 Rev. 2 technical references, mappings, and assurance content remain unchanged. Corrected the §5.1 hardware-Purge verification description to state that pre/post-erase snapshots are taken at 5 fixed reference LBAs (first, 25%, 50%, 75%, last) rather than random LBAs, matching the implementation; made the "≥1 block changed" pass condition explicit. Aligned the §9 Document-Control version and review date with the document header. Added host system-specification fields to the §7 certificate field list. No change to the erasure methodology, supported media, or conformance scope.

Version 1.4 — 2026-07-28
Aligned the statement with the v2.0.x evidence architecture following a full code audit. Local artifact reclassified as a sanitization evidence report; §5.2 rewritten — §4.5.2 organizational validation and certificate issuance moved to Retsu - Portal, with the local automated result recorded as a technical assessment carrying no standard claim. §4.2 rewritten: added NVMe Sanitize Overwrite (SANACT=3) as an operative technique; documented Sanitize Status Log acceptance criteria (SSTAT, Global Data Erased, SCDW10 linkage) with per-run fresh-run proof; reclassified the pre/post

snapshot comparison as supplementary, non-authoritative evidence. §4.4 rewritten: both NVMe Cryptographic Erase techniques documented as implemented but administratively disabled fail-closed pending model/firmware-specific cryptographic evidence; removed the ATA SED implicit-CE claim (no ATA cryptographic-erase mode exists). §4.3: scope corrected to rotational SATA media only (SATA SSD Purge refused fail-closed); added storage-interface establishment, dual ATA capability probes, and mandatory HPA/DCO exposure with post-checks; corrected frozen-drive handling and conditional password cleanup. §5.1: corrected sampling description (first and final 4 KiB regions fixed, remainder pseudorandom; read errors fail; zero-check limited to zero-final methods) and hardware-Purge verification (controller evidence authoritative; snapshot comparison NVMe-only and supplementary). §7 updated for evidence-report outputs, the bootable on-drive evidence presentation with verifiable SHA-256 digest, and accurate tool-version recording. §8 extended with the CE-disabled and rotational-only-ATA non-claims. No change to the Clear methodology. Post-draft code alignment: documented the marker-backed Global Data Erased controller-anomaly acceptance path ("completed with controller anomaly") and the sanitize-action match requirement in §4.2/§5.1/§7; removed the local validation-status and certificateEligible fields from §5.2/§7 to match the current evidence schema (organizational validation status is Portal-only); aligned all applicable-from version fields to v2.2.4.

SIGNATURE

I attest that the information provided in this statement is accurate to the best of my knowledge.

Signed: 

Ibrahim Dehhani

Founder, Dehhani Ltd

Date: 28th July 2026