DSU – ERASURE

NIST SP 800-88 REV. 2 CONFORMANCE STATEMENT

Product: DSU - Erasure
Vendor: Dehhani Ltd
Applicable from version: 1.4.0
Document Version: 1.2
Document Date: 2026-04-10
Author: Ibrahim Dehhani, Founder, Dehhani Ltd

1. PURPOSE

This document is a vendor self-attestation that the data sanitization functions implemented in DSU - 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).

DSU - 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This statement covers DSU - Erasure v1.4.0 and all subsequent versions unless superseded by a later revision of this document.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: Yes (ATA Secure Erase)

Notes: Operator warned that software overwrite cannot reach wear-levelled blocks; Purge recommended.

NVMe Solid State Drive (SSD)
Clear: Yes (with warning)
Purge: Yes (NVMe Sanitize Block Erase, NVMe Sanitize Crypto Erase, NVMe Format Crypto Erase)
Notes: Operator warned that software overwrite cannot reach wear-levelled blocks; Purge recommended

USB flash drives
Not supported — not a target platform for DSU – Erasure

eMMC / embedded storage
Not supported — not a target platform for DSU - Erasure

Sanitization Methods in the DSU - Erasure Operator Interface:

NIST Clear (SP 800-88) — maps to SP 800-88r2 Clear (§3.1.1)
NIST Purge (SP 800-88) — 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." DSU - 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 technically equivalent to a single-pass NIST Clear when applied to magnetic media, since both overwrite the addressable storage with a fixed pattern followed by a zero pad.

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 DSU - 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 DSU - 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."

DSU - Erasure implementation:

DSU - Erasure's Clear sanitization module performs a single-pass overwrite of every user-addressable logical block address (LBA) on the target device with all-zero data. The overwrite is performed using a standard write interface at the block-device level, covering the full addressable capacity of the drive in a single sequential pass.

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. DSU - 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."

DSU - Erasure implementation:

DSU - Erasure queries the NVMe controller's Sanitize Capabilities (SANICAP) and Format-NVM-Attributes (FNA) registers and attempts the following methods, in priority order, falling back only on hardware non-support. Each technique 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 NVMe Specification §5.21, action Block Erase. Issues the NVMe Sanitize command instructing the controller to perform a media-level erase of all user data blocks. SP 800-88r2 §3.1.2 explicitly lists "block erase" among the acceptable logical Purge techniques.

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

Aligned with NVMe Specification §5.21, action Crypto Erase. Issues the NVMe Sanitize command instructing the controller to destroy the symmetric data-encryption key, cryptographically erasing all user data. Conforms to SP 800-88r2 §3.2 (Use of Cryptography and Cryptographic Erase) and §3.1.2.

3. NVMe Format — Cryptographic Erase (ses=2)

Aligned with NVMe Specification §5.13, Secure Erase Setting 2 (Cryptographic Erase). Issues the NVMe Format command with the Cryptographic Erase secure-erase setting to all namespaces. Conforms to SP 800-88r2 §3.2. Note: Secure Erase Setting 1 (User Data Erase) is not claimed as Purge by DSU - Erasure, because it permits an FTL-only reset that does not satisfy SP 800-88r2 Purge requirements.

After each successful command, DSU - Erasure performs a post-erase block snapshot comparison against a pre-erase snapshot to confirm that user data has actually been destroyed. If the snapshots are identical, DSU - Erasure treats the erase as failed and proceeds to the next method or fails the job entirely. DSU - 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 method that succeeded is recorded on the erasure certificate (e.g., "NVMe Sanitize Crypto Erase (sanact=4) — NIST SP 800-88 Purge").

4.3 NIST Purge — SATA HDDs and SATA SSDs

DSU - Erasure implementation:

DSU - Erasure issues standard ATA Security feature-set commands to perform hardware-level erasure on SATA drives:

1. Detect frozen state

DSU - Erasure checks the drive's ATA Security feature set status. If the drive reports "frozen" (a common state after BIOS initialisation), DSU - Erasure attempts an ACPI suspend/resume cycle to clear the frozen state. If the drive remains frozen, the operation fails with a clear diagnostic to the operator.

2. Set temporary user password

A temporary ATA security password is set on the drive to enable the Secure Erase command set.

3. 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 HDDs and SSDs and is accepted by SP 800-88r2 §3.1.2 as a logical Purge technique.

4. Fallback to Standard Secure Erase

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

5. Cleanup

On any failure path, DSU - Erasure disables the temporary password so the drive is left in a recoverable, non-locked state.

The exact method used is recorded on the certificate (e.g., "ATA Enhanced Secure Erase — NIST SP 800-88 Purge").

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.

DSU - Erasure implementation:

DSU - Erasure invokes Cryptographic Erase via the storage device's own firmware on Self-Encrypting Drives (SEDs). The target key sanitized in every CE operation is the symmetric data-encryption key held inside the drive controller — the first of the four categories enumerated in §3.2.3:

NVMe SED: via the NVMe Sanitize Crypto Erase command (sanact=4) and the NVMe Format Cryptographic Erase command (ses=2)

ATA SED: implicit when Enhanced Secure Erase is issued against a drive with hardware encryption

DSU - Erasure does not perform software-side cryptographic erase, and does not issue Cryptographic Erase against drives that lack hardware encryption support — the drive's capability registers are checked first to confirm support.

§3.2 pre-condition compliance: SP 800-88r2 §3.2.2 specifies that no sensitive data should have been stored on the ISM in plaintext form prior to CE. DSU - Erasure surfaces this consideration to the operator implicitly: if a customer is sanitising a drive that contained plaintext data prior to encryption, the operator should select NIST Purge (which on supported drives executes the Block Erase technique in addition to or instead of CE) rather than relying on CE alone.

§3.2.4 cryptographic implementation quality: SP 800-88r2 §3.2.4 recommends that organisations relying on CE either obtain independent validation of the underlying cryptographic implementation or ask the ISM vendor for the relevant assurances (entropy quality, encryption algorithm strength, key sanitization technique, key wrapping). For SEDs, this assurance comes from the drive vendor's published cryptographic conformance (commonly TCG Opal/Pyrite or FIPS 140-2/-3 validation). DSU - Erasure does not perform cryptographic implementation testing of the target drive; it issues the standard interface command and relies on the SED's own conformance.

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.

DSU - Erasure implements both activities:

5.1 Sanitization Verification (§4.5.1)

DSU - Erasure performs randomised block-sample inspection after every erase operation:

Software overwrite (NIST Clear, HMG IS5 Baseline, Zero Fill):

Read 10 random 4 KB blocks (including LBA 0 and the final LBA). All bytes in every sampled block must equal zero. Any non-zero byte constitutes a verification failure.

Hardware Purge (NVMe Sanitize, NVMe Format, ATA Secure Erase):

(a) Pre-erase snapshot at 5 random LBAs.

(b) Post-erase snapshot at the same LBAs.

(c) Snapshot comparison must show data has changed.

(d) Post-erase readability check at 10 random LBAs.

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. DSU - Erasure's randomized sampling exceeds the SP 800-88r2 minimum and is an additional defensive measure beyond what the standard requires.

5.2 Sanitization Validation (§4.5.2)

The validation decision in DSU - Erasure is automatic and deterministic. If the verification step detects any failures (non-zero data where zeros are expected, or unchanged data after a hardware erase), DSU - Erasure marks the job as failed, records the failure count and notes on the certificate, and surfaces the failure to the operator. If verification passes, DSU - Erasure marks the job as complete. The operator can then make a final acceptance or rejection decision based on the certificate, in accordance with their organization’s media sanitization program.

DSU - 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

DSU - 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 a software-overwrite method on a detected solid-state drive, DSU - Erasure displays a warning recommending NIST Purge instead, citing the SP 800-88r2 limitation on overwriting wear-levelled blocks.

Frozen drive guidance: If an ATA drive's security feature set is frozen and cannot be unfrozen, DSU - Erasure instructs the operator to either physically reseat the drive or fall back to NIST Clear.

Hard fail on Purge unavailability: If all hardware Purge methods fail on an NVMe drive, DSU - Erasure does not silently fall back to a software overwrite; it fails the job and surfaces a diagnostic message so the operator can make an informed decision.

7. ERASURE CERTIFICATE (§4.6, APPENDIX C)

For every successful erasure, DSU - Erasure generates a certificate of sanitization. SP 800-88r2 §4.6 and Appendix C specify the minimum fields a Certificate of Sanitization should record. DSU - Erasure's certificate records the following:

Manufacturer — Drive manufacturer

Model — Drive model number

Serial number — Drive serial number

Media type — Detected media type (HDD / SATA SSD / NVMe SSD)

Sanitization method — The selected erasure method, mapped to the NIST category (Clear / Purge)

Sanitization technique — The specific ATA or NVMe command that was issued

Tool used, including version — DSU - Erasure, with underlying tool versions logged

Verification method — Random-block zero verification (for Clear) or pre/post snapshot comparison (for Purge)

Validation result — Pass/fail status, sample count, blocks verified, failure notes

Date/time — Start and end timestamps with total duration

Person performing sanitization — Operator/technician identification (when configured)

Signature — Operator signature line on the printable certificate

Certificates are produced in both human-readable text and HTML formats. They are:

Persisted locally to the device's erasure-reports store for immediate access.

Submitted to the DSU Portal (devicesetup.app) for centralised audit storage and retrieval by the customer's account administrators.

Written to a recovery partition on the erased drive (when supported), so the certificate physically travels with the device as proof of sanitization.

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. DSU - 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. DSU - 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; DSU - Erasure surfaces it to the operator and recommends NIST Purge for SSDs.

5. DSU - 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. DSU - 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. DSU - Erasure does not address partial ISM sanitization (SP 800-88r2 §4.2). All DSU - Erasure methods sanitize the entire user-addressable area of the drive.

9. DOCUMENT CONTROL

Document ID: *DSU-NIST-800-88-CONF-001*
Standard version: *NIST SP 800-88 Revision 2 (September 2025)*
Applicable from: *DSU - Erasure v1.4.0*
Document version: *1.2*
Last reviewed: *2026-04-10*
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 DSU - Portal certificate submission to Section 7. Added revision history table. Branded as DSU - Erasure / Dehhani Ltd. Changed version field to "Applicable from" model.

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: 10/04/2026