DATA SAFE
SOLUTIONS

TECHNICAL BRIEFING · SEPTEMBER 2026

A certified erasure that leaves the data behind.

How the standard purge hierarchy fails on flash media, and why it creates a standing UK GDPR Article 5(2) exposure across the public sector estate.

CLEAR, PURGE AND DESTROY

The category depends on the media, and on flash the wrong one is being certified.

Data sanitisation renders data on storage media irrecoverable before a device is reused, resold or disposed of. NIST SP 800-88 and IEEE 2883 define three categories. This briefing concerns what happens on modern flash storage when the media-appropriate method is refused and a weaker one is substituted in its place.

Clear

Overwrite through the drive's normal read and write interface. Reaches user-addressable locations only. Adequate for magnetic media, not for flash.

Purge

Media-appropriate commands such as cryptographic erase, block erase or sanitize. Also addresses the locations the normal interface cannot reach. The correct category for flash.

Destroy

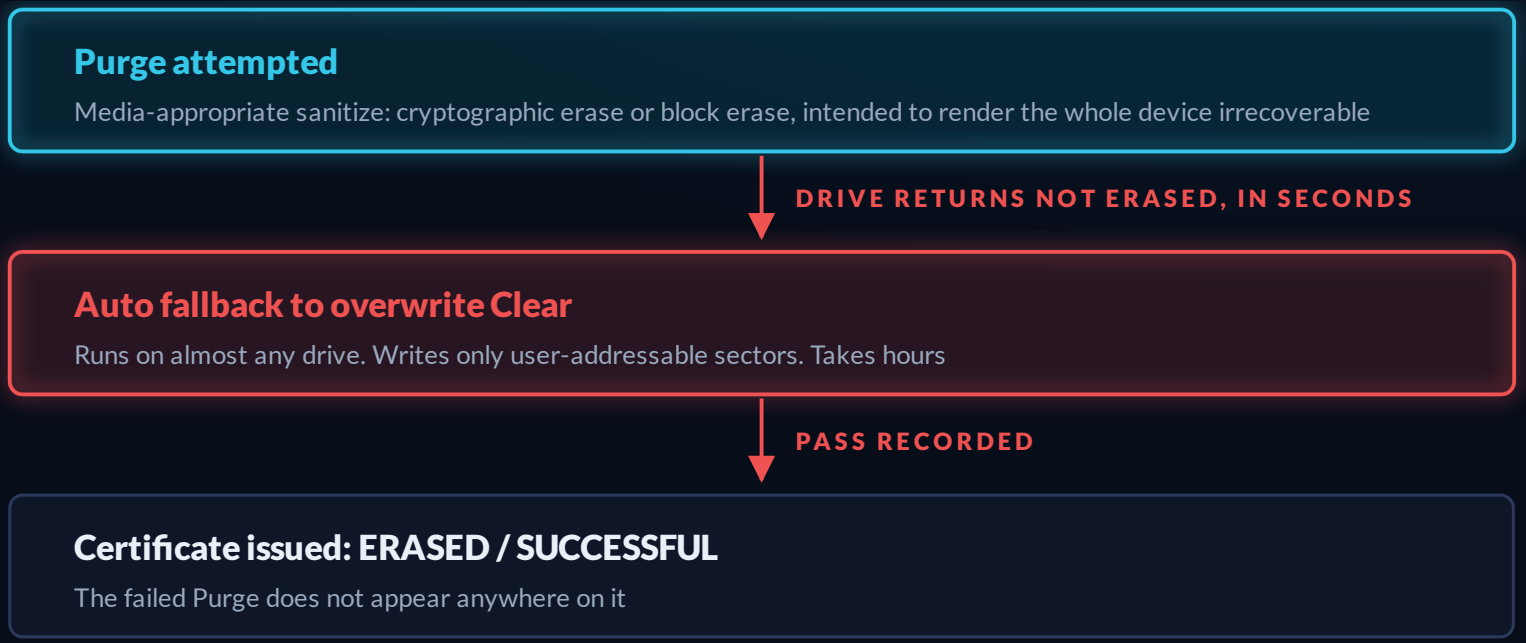
Physical destruction of the media. The remaining option where a Purge cannot be completed or verified.

On flash media the tool attempts Purge, the drive refuses it, the tool substitutes Clear, **and the device is certified as erased.**

ONE · WHAT WAS CONFIGURED

Try a Purge. On failure, quietly do less.

A fixed hierarchy runs on every device. The selected Purge method is attempted, and if the drive refuses it, the tool falls back automatically to overwrite and certifies the result. The method has already been chosen before the individual drive is processed. Some platforms subsequently check whether that chosen method is supported; others simply attempt it. Neither determines which sanitisation method is correct for that individual device. No route to destruction.



The selected Purge method was attempted, the drive refused it, a lesser method ran in its place, **and the result was certified a success.**

TWO · WHY THE PURGE FAILED

Every drive has a different lock. It tried one key on every door.

Four steps, no jargon. This is what the erasure logs are actually recording.

Every drive has a different lock

There is no universal erase command. The instruction that destroys the data depends on the individual drive, its controller and its firmware.

It tried one key on every door

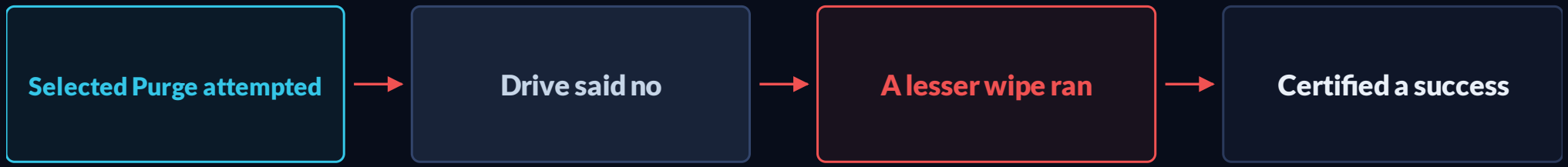
The tool starts with a method already chosen in advance. On some platforms that method is checked for support before execution; on others it is simply attempted. What neither does is determine the correct method from that individual device. On drives taking a different lock, the key did not fit and the drive refused within seconds.

So it swept the floor instead

It fell back to overwrite, which reaches only the user-addressable sectors. The drive keeps whole regions outside that view, and the method that ran does not reach them.

And signed it off as done

The certificate records a success. The failed Purge never appears, so the customer cannot tell this drive from one that was properly sanitised.

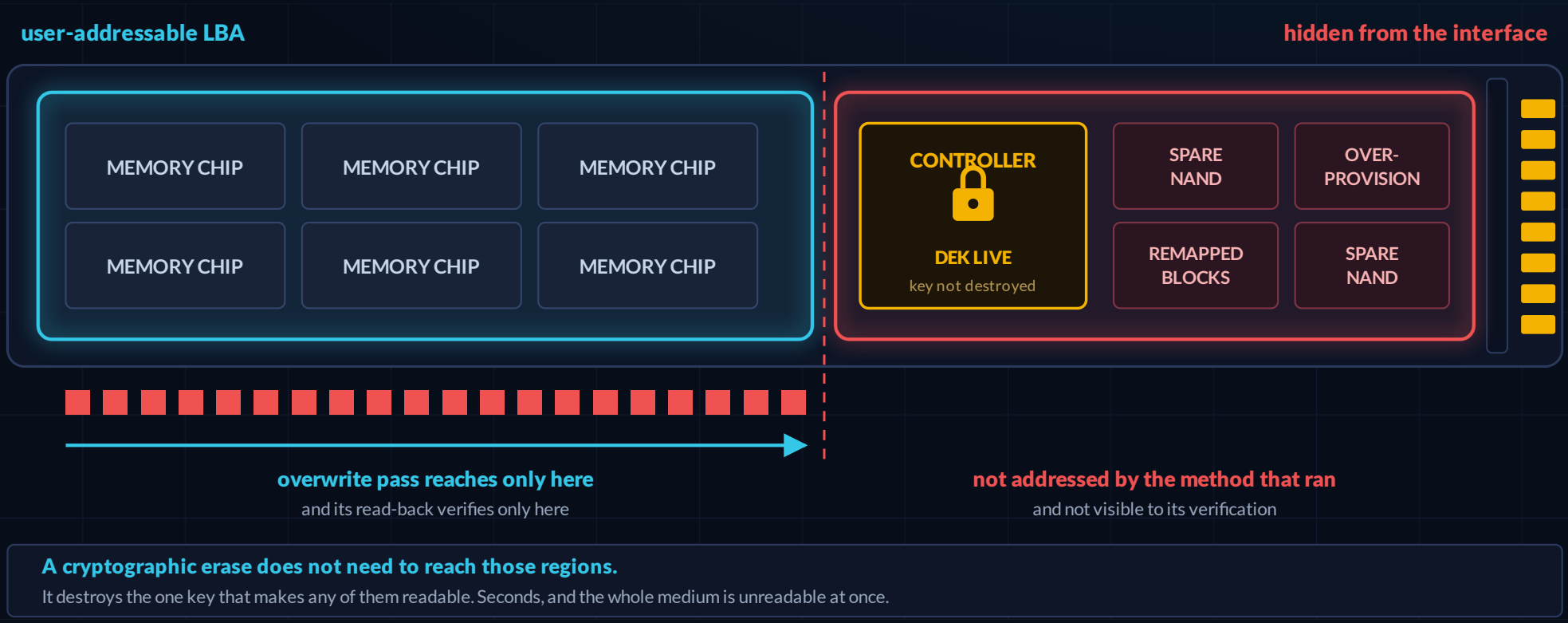


A device recorded as erased may be one on which the media-appropriate method never ran, **and on the face of the record it is indistinguishable from one that was properly sanitised.**

THREE · WHERE THE DATA ACTUALLY LIVES

NVMe SSD self-encrypted drive
Form factor M.2 2280

The data sits in the memory chips. The controller holds the device encryption key and silently relocates blocks into spare and over-provisioned area that the operating system never sees. M.2 2280 denotes the form factor only; 2230, 2242, 2260 and others are equally common.



A cryptographic erase does not need to reach those regions.
It destroys the one key that makes any of them readable. Seconds, and the whole medium is unreadable at once.

THREE · THE PEER-REVIEWED POSITION

The method and the verification share one boundary.

Neither can reach past the host interface, and on flash that is where the residue sits. A read-back, however thorough, confirms only the region the overwrite could already reach.

PEER-REVIEWED ACADEMIC WORK

Carlo Meijer and Bernard van Gastel, Radboud University Nijmegen, ***Self-Encrypting Deception: Weaknesses in the Encryption of Solid State Drives*** **(2018).** Laboratory analysis of shipping self-encrypting drives from Crucial, Micron, Samsung, Western Digital and SanDisk. Two findings bear directly on the previous page. On several drives **the media encryption key was not cryptographically bound to the user credential**, so the data could be decrypted without it. And **wear levelling left recoverable copies of superseded key material in the flash after the key had been changed**, because writing a new key does not erase the physical location holding the previous one. That is the same architectural behaviour as the residual data problem, applied to the key itself. Assigned CVE-2018-12037 and CVE-2018-12038, tracked by CERT/CC as VU#395981. **We have identified no published work retesting this failure class on current-generation drives.**

Wrong command for the drive

Rejected in seconds. The Purge never ran.

Key never destroyed

The device encryption key stays live in the controller.

Whole regions not addressed

Remapped, spare and over-provisioned area is outside the reach of the method that ran.

Certificate reads Erased

Nothing on its face distinguishes this device from one properly sanitised.

A cryptographic erase does not need to reach those regions. **It destroys the one key that makes any of them readable.**

FOUR · THE CASE FOR CHANGE

Why the standard configuration no longer holds.

The fixed hierarchy was a sound engineering answer to the problem as it stood when it was designed. Four assumptions supported it. On current media, and under the standards now in force, none of them still do.

Assumption: the batch is uniform hundreds of the same model arrive together	Storage is internal and invisible on the asset register. An identical model line is built with whatever drives were sourced at the time, so NAND vendor, controller, self-encrypting implementation and firmware all vary inside the same chassis. **A per-model or per-batch policy is invalid by construction.**
Assumption: no capability data exists matching would need an external map	The drive reports its own capabilities on request, and the tool already queries the device during identification. **The data needed for correct selection is already in hand at the point of decision.**
Assumption: it removes operator judgement a consistency control	Automated pre-selection removes more judgement, not less, and records why each method was chosen for each unit. **This assumption argues for capability matching rather than against it.**
Assumption: throughput requires a fallback the line must never stall	The decisive point, and it runs the other way. Cryptographic erase completes in seconds where the overwrite fallback takes hours. **Matched selection is the faster line, not the slower one**, and it returns more drives to resale rather than fewer.

NIST SP 800-88 Revision 2 became final in September 2025 and defers method selection to IEEE 2883. IEEE 2883.1-2025 requires verification that the selected method actually completed. **A configuration that resolves an unverified result toward a pass was defensible under the old framework. It is not under this one.**

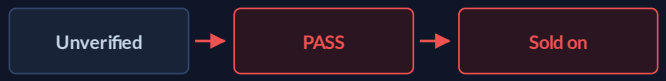
FIVE · WHICH WAY DOES IT FAIL?

Both systems meet devices they cannot verify. Only the next step differs.

Controlled firmware validation testing with a UK public sector customer, May and June 2026, with baseline and post-update firmware captured on each unit.

STANDARD CONFIGURATION

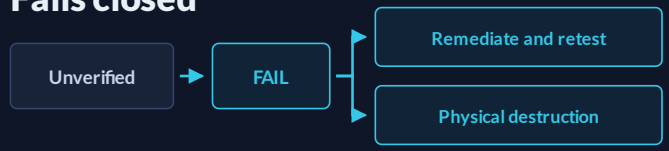
Fails open



The system resolves its own uncertainty in favour of a pass and a resaleable asset, and the doubt never reaches the customer.

DSS SMART WIPE

Fails closed



Overwrite fallback is removed entirely. Nothing is certified on a substitute.

HOST	STORAGE MODEL	INTERFACE	RECORDED SANITISATION LEVEL	DATE
ThinkCentre M70q	Samsung MZALQ256HAJD	NVMe PCIe, 256GB	**NIST 800-88 Clear**	2026-06-08
ThinkCentre M720q	Samsung MZ7LN128HAHQ	SATA SSD, 128GB	**NIST 800-88 Clear**	2026-06-10
ThinkPad X13 Gen 1	Kioxia KBG40ZMT128G	NVMe PCIe, 128GB	**NIST 800-88 Clear**	2026-05-28
ThinkPad X13 Gen 1	Kioxia KBG40ZMT128G	NVMe PCIe, 128GB	**NIST 800-88 Clear**	2026-05-26
ThinkPad X390	SK hynix HFM128GDHTNG	NVMe PCIe, 128GB	**NIST 800-88 Clear**	2026-05-27

The firmware update resolved the purge failure. **These were remediable defects, not hardware limitations**, and under a fallback configuration every one would have shipped with the defect unrecorded and unfixed.

SIX · THE THREAT MODEL

No intrusion is required. The devices leave custody legitimately.

Decommissioned equipment is freely acquirable on the secondary market. Acquire in bulk, bypass the logical view, recover what the interface never showed, and correlate across departments.

I
Acquire

Bulk buy decommissioned public sector equipment on the secondary market.

II
Bypass the interface

Controller, diagnostic or specialist NAND-reconstruction techniques, ignoring the logical view entirely.

III
Recover

Where the media key remains live, reconstruct remapped and spare-area content and carve what is there.

IV
Aggregate

Fuse many devices into one indexed corpus and correlate across departments.

ONE DEVICE IN ISOLATION

Fragments on one ex-government laptop.

Expensive to extract for a handful of stale files.

On its own, a near-worthless target.

THE ESTATE IN AGGREGATE

Thousands, across every department.

Assembled, that is a strategic intelligence problem built entirely from certified disposals.

The exposure is not per device. It is cumulative.

Each certified failure is one more tile, and the estate gives up the mosaic quietly, over years.

SEVEN · THE REMEDY

Pre-selection by device capability.

Keep the throughput. Keep the removal of operator judgement. Change only when the method is chosen: decide it from the drive itself, before erasure starts, rather than discovering it by failure afterwards.

	CURRENT: DECIDE BY FAILURE	PRE-SELECTION: DECIDE BY CAPABILITY
ONE	Run a fixed command, blind to the device	Interrogate first. Read each drive's identity, interface, self-encrypting status, firmware and sanitize capability set
TWO	The drive rejects it and returns Not Erased	Bind per unit. Match that profile to the one media-appropriate method, automatically. Never per model, never per batch
THREE	**Silently fall back to overwrite**	**Execute only the matched method. No hierarchy and no substitution**
FOUR	**Certify as erased. The failure signal is discarded**	**Verify the outcome at the device. Known verification data is established before sanitisation, then recovery of that same data is attempted afterwards. Where the outcome cannot be proven, fail closed**
FIVE	No route to destruction	Divert on any failure, to remediation and retest or to physical destruction

On a modern self-encrypting drive the matched method is cryptographic erase: seconds to run, verifiable, and it leaves the drive fully resaleable. **Correct pre-selection increases the number of devices safely returned to use.**

EIGHT · THE PROPOSITION

Better outcome, faster line, more resale.

This is not a case for destroying more equipment or slowing throughput. Capability-led selection improves both, and it produces the evidence the current framework expects.

More drives returned to resale

A failed Purge under the current model is invisible. Under capability-led selection it is identified, and in many cases resolved by firmware update and retest rather than destruction.

A faster process, not a slower one

Cryptographic erase completes in seconds where an overwrite pass runs for hours. Matching the method to the device removes the longest single operation on the line.

Evidence that meets the standard

Per-device records of capability, method selected, execution and verification. What IEEE 2883.1-2025 asks for, and what a batch certificate cannot provide.

No double charging

You are not billed for a failed selection and then billed again for the fallback overwrite that follows it. Monthly, in arrears, for what was processed.

THE PROTECTED DIFFERENCE

No single step is the invention. The integrated per device chain is patented and published, **GB2638704**, with a related US filing.

1

Joint validation

Run an agreed sample of live intake through both configurations and compare outcomes device by device.

2

Shared findings

Review the Purge failure rate, the recovery rate after firmware remediation, and the throughput difference.

3

Commercial discussion

Agree how the capability-led engine is integrated, on what terms, and over what timeframe.

> The technical position is not in dispute. The question is which way the process should fail when a device cannot be verified, **and every current standard answers that the same way.**

Sources. Operational erasure reports from large ITAD providers, redacted. Firmware validation testing with a UK public sector customer, May and June 2026, anonymised. NIST SP 800-88 Rev 2 (2025). IEEE 2883-2022 and 2883.1-2025. Meijer and van Gastel (2018), *Self-Encrypting Deception*, Radboud University Nijmegen, CERT/CC VU#395981. ICO case IC-471076-R5B2.

Data Safe Solutions Ltd, ADISA certified, NIST SP 800-88 aligned · Port of Liverpool Building, Mann Island, Liverpool L3 1BY · 0151 440 3200 · hello@datasafe360.com · datasafe360.com