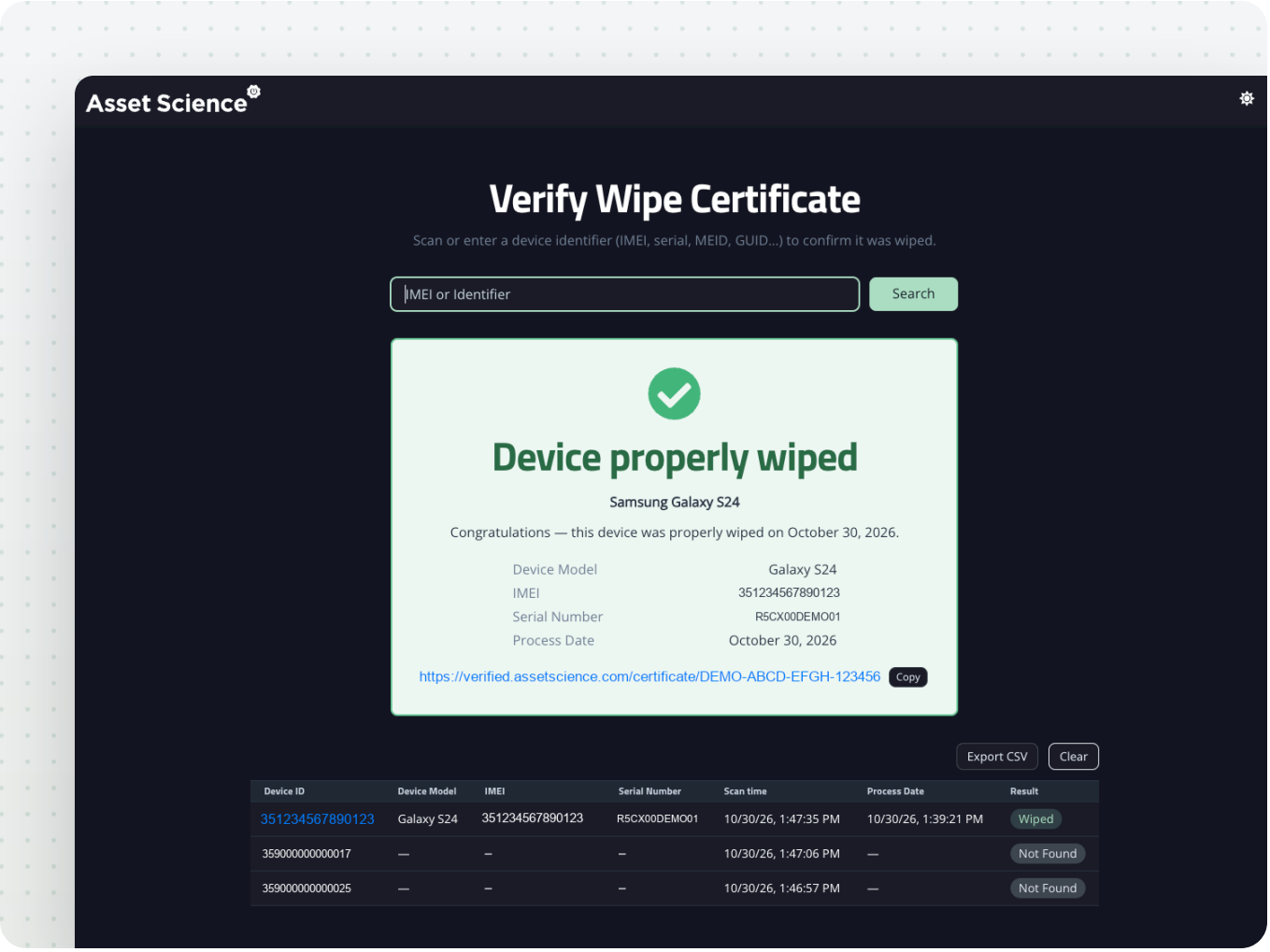
PUBLIC WEB CERTIFICATION

The evidence leaves your building.

Anyone holding an IMEI or a serial can check what happened to a device you processed at verified.assetscience.com. No account, no sign-in. A wipe and diagnostic certificate, a shareable link, a PDF, and batch export for the pallet.



AUDIENCE

Operations, compliance & IT leaders at device processors

LOOKUP

IMEI · Serial · MEID · GUID

PUBLIC CERTIFICATES

verified.assetscience.com/verify

AT A GLANCE

The eight questions every buyer asks.

This product is the certificate, not the test bench. It publishes what the Asset Science platform recorded about a device, to anyone who can type its identifier.

CERTIFICATE

Yes

Public web lookup by IMEI, serial, MEID or GUID at verified.assetscience.com, a shareable certificate link, a downloadable PDF, and certificate PDFs generated in batch.

ADISA CERTIFIED

AAL 4

Certificates from **Pro-Diagnostics (PDD) and MacRestore** carry the ADISA assurance level 4 mark. Pro-Diagnostic PC is not ADISA certified; its erase report names NIST 800-88 methods instead.

TYPE OF WIPE

NIST 800-88

The certificate states the **content clearing method**: on devices with full-disk encryption the key is destroyed; on unencrypted devices overwrite is applied. Factory reset is confirmed as a status tile.

GUIDED USER TESTING

Not applicable

Testing happens in the diagnostic products. The certificate **reports their results**; it does not run tests of its own.

TYPE OF TESTS

Reported, not run

Diagnostic results with pass and fail counts, battery health, and device status checks such as GSMA blacklist, factory reset and eSIM, as recorded during processing.

MAIN FEATURES

4

Public lookup without an account. Shareable link and PDF. **Batch CSV export and batch PDF certificates.** Per-customer controls over what is published.

PLATFORMS SUPPORTED

Any browser

The lookup and the certificate are **web pages**. Nothing to install for the buyer, the auditor or the end owner. Records come from the Asset Science platform.

DATA ANALYTICS AND API

CSV

Scanned batches export to CSV from the lookup screen; bulk lookup takes a CSV of up to 30,000 identifiers. The underlying record stays in Control Center with its full data export.

1

Process

The device is tested and cleared on the platform. One record per unit.

2

Publish

Your account decides what goes public: search, page, PDF.

3

Look up

Anyone types or scans an identifier. No account.

4

Verify

The certificate opens, with a link to share and a PDF to keep.

One record, three ways to reach it. Search by identifier on the public page, open the shareable certificate link, or scan the QR code on the label. All three resolve to the same certificate for that device.

WHY A PUBLIC CERTIFICATE MATTERS

A record nobody outside your building can read is an assertion.

Every device you process can be looked up by IMEI or serial on a public page, by your buyer, your client's auditor, or the person who ends up owning the phone.

THE BUYER

Opens the evidence from the file you sent.

Certificate links travel inside exported reports. A buyer receiving a lot does not take the spreadsheet's word for it; each row points at a page they can open themselves.

THE AUDITOR

Reads vocabulary they already know.

The certificate names the content clearing method, shows GSMA blacklist and factory-reset status, and carries the ADISA mark where the processing product holds it.

THE END OWNER

Checks the phone in their hand.

The QR code on the label resolves to the same certificate. Whoever ends up with the device can confirm it was cleared, and when, without asking anyone.

Not Found means not found. A device nobody processed comes back Not Found rather than a reassuring blank. The lookup never implies a wipe it has no record of.

ADISA

Certified to ADISA assurance level 4, stated at its scope.

Pro-Diagnostics and MacRestore are certified to ADISA assurance level 4, independently tested by the ADISA Research Centre under its Product Claims Test. Certification applies to the products named. Pro-Diagnostic PC is not certified, so no certified-erasure claim is made for computers; its reports name NIST 800-88 methods per drive.

NIST 800-88 REV. 2

Clear and Purge are not interchangeable.

Each drive gets the stronger method it is actually capable of, and the method used is named on the erase report alongside that drive's serial number.

IEEE 2883

The standard's own terminology.

Sanitisation terminology and verification expectations are aligned to the current standard, so an auditor reading our report is reading vocabulary they already know.

THE LOOKUP

Anyone can check a device, without an account.

Scan or type any identifier: IMEI, serial, MEID or GUID. The result links straight to the certificate for that device.

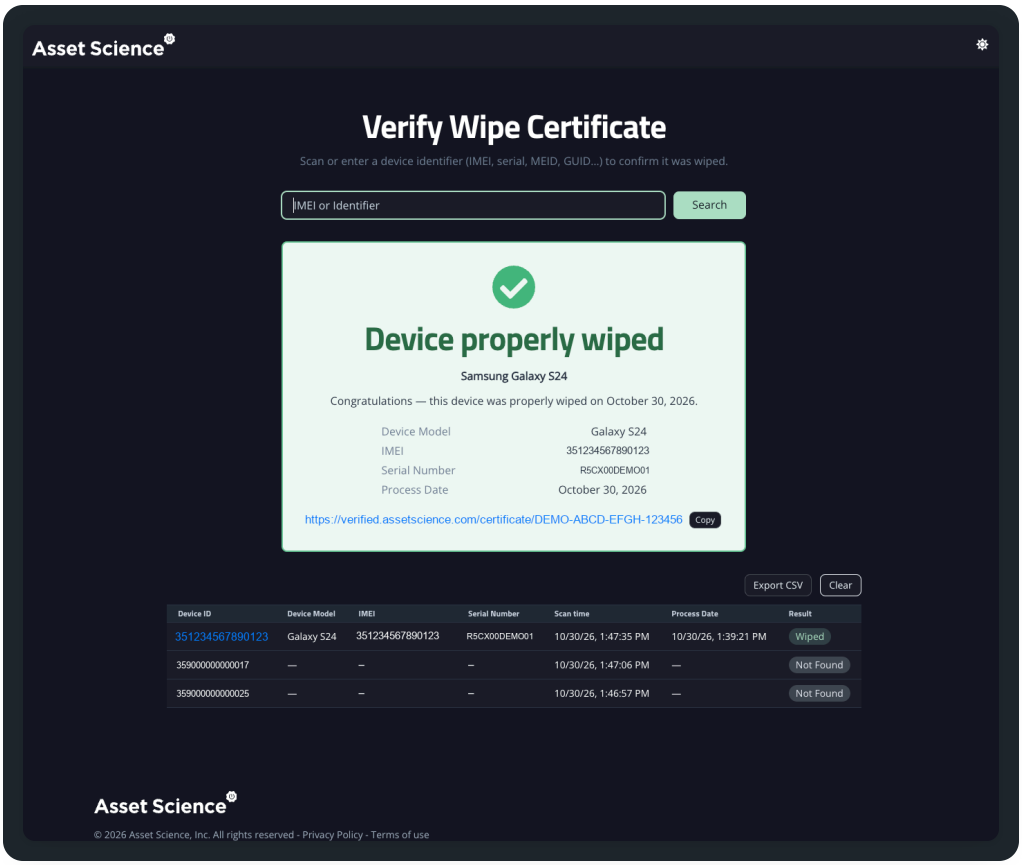


FIG. 1 verified.assetscience.com/verify. A wiped device returns a result card with model, IMEI, serial and process date, and a certificate link with a Copy button. Below, the scanned batch with Export CSV. Two identifiers nobody processed come back Not Found. Identifiers shown are synthetic.

1

Scan or type

One search box. A barcode scanner or a keyboard, any supported identifier.

2

Read the result

Device properly wiped, with model, IMEI, serial and the process date. Or Not Found.

3

Copy the link

The certificate link opens for anyone holding it, if your account allows it.

4

Export the batch

Every scan in the session lands in a table. Export CSV takes the whole batch.

Nothing to install, nothing to sign up for. The page is open to anyone with an identifier. What they can see of a device you processed is decided by your account's publishing controls, described on page 6.

THE CERTIFICATE

What was cleared, how, and what the device tested as.

The page behind the result, downloadable as a PDF by anyone holding the link. One certificate per device, with its own certificate ID.

HEADER AND RESULT

Certificate ID, session, model, IMEI, outcome.

A banner states the outcome in one line: Data Cleaning & Diagnostics Complete, Fully Functional. Wipe-only processes carry a Data Cleaning Certificate instead, with a Fully Wiped banner.

CONTENT CLEARING METHOD

How the data was removed, and the ADISA mark.

The encryption type is identified; on full-disk-encrypted devices the key is destroyed, on unencrypted devices overwrite is applied. The ADISA assurance level 4 badge sits under the statement.

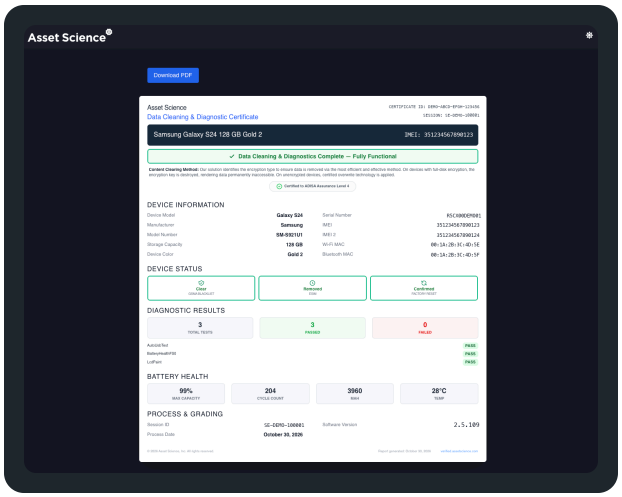


FIG. 2 verified.assetscience.com → Certificate. A Data Cleaning & Diagnostic Certificate with the Download PDF button above it. Identifiers, MAC addresses and session IDs are synthetic.

DEVICE INFORMATION

Ten identity fields.

Device model · Manufacturer · Model number · Storage capacity · Device color · Serial number · IMEI · IMEI 2 · Wi-Fi MAC · Bluetooth MAC

DEVICE STATUS

Checks that ran, as tiles.

Green when a check ran and passed, red when it ran and failed, amber N/A when it did not run. Checks include activation, Find My, GSMA blacklist, MDM, eSIM, factory reset and parts. Locks are reported, never removed.

DIAGNOSTIC RESULTS AND BATTERY

Counts, then every test by name.

Total, passed and failed, followed by each test with its PASS or FAIL. Battery health gives maximum capacity, cycle count, capacity in mAh and temperature.

PROCESS AND GRADING

Who, when, on what software.

Session ID, process date and the software version that produced the record. The footer carries the generation date and the verification site.

The certificate reflects the recording, nothing more. A check that did not run shows N/A rather than a pass. A process that failed before the wipe step shows Factory Reset as Failed, and the banner reads Process Failed. A failed device is never quietly certified.

YOU DECIDE WHAT IS PUBLIC

Three switches per customer account, set in Control Center.

Publication is opt-in. The certificate page and the PDF are separate switches, so turning the page off does not by itself make the PDF private. That is a second control, deliberately.

CONTROL	WHAT IT ALLOWS
Publish results to public search	Anyone can look up a device you processed by IMEI or serial and see its data-wipe and diagnostic results.
Allow public certificate links	Anyone holding a certificate link can open the certificate page without signing in. Also controls the Public Certificate button in Device History and the certificate links in exported reports.
Allow public PDF download	Anyone holding a certificate link can download the certificate as a PDF without signing in. A separate switch from the page above.

EVIDENCE BY THE BATCH

Nobody clearing a pallet wants to open one certificate at a time.

- **Export a scanned batch to CSV** straight from the lookup screen.
- **Bulk device lookup** from a CSV of up to 30,000 identifiers.
- **Certificate PDFs generated and sent in batch**, not one device at a time.
- **Certificate links travel inside exported reports**, so a buyer can open the evidence from the file you send them.

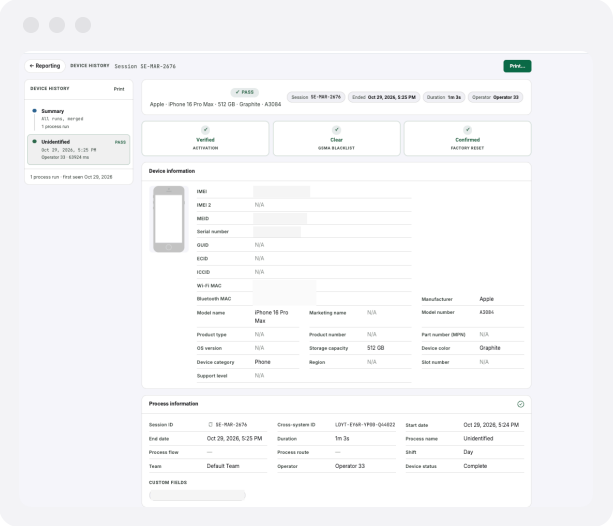


FIG. 3 Control Center → Device History. The same evidence as tiles on the device's own record: activation verified, GSMA clear, factory reset confirmed, above the identifier block and process information. Identifiers are synthetic.

Inside and outside match. What the public certificate shows is what Device History holds in Control Center. There is one record per device, and the public page is a view of it, not a second copy.

PUBLIC VERIFICATION

Certification claims in this market are routinely stretched past their scope.

Ours are stated at their scope, with the certified products named. And the record itself is public: a buyer, an auditor or an end owner can read it without taking our word, or yours, for it.

Try the lookup on a device you processed.

Start a free trial, process a device, and look it up on the public page. Then decide, per account, what the rest of the world gets to see.

FREE TRIAL
onboarding.assetscience.com

PUBLIC CERTIFICATES
verified.assetscience.com/verify

WEB
assetscience.com

© 2026 Asset Science. Screenshots are from production builds; device identifiers, session IDs, operator names and customer data shown are synthetic. Product names and marks belong to their respective owners.