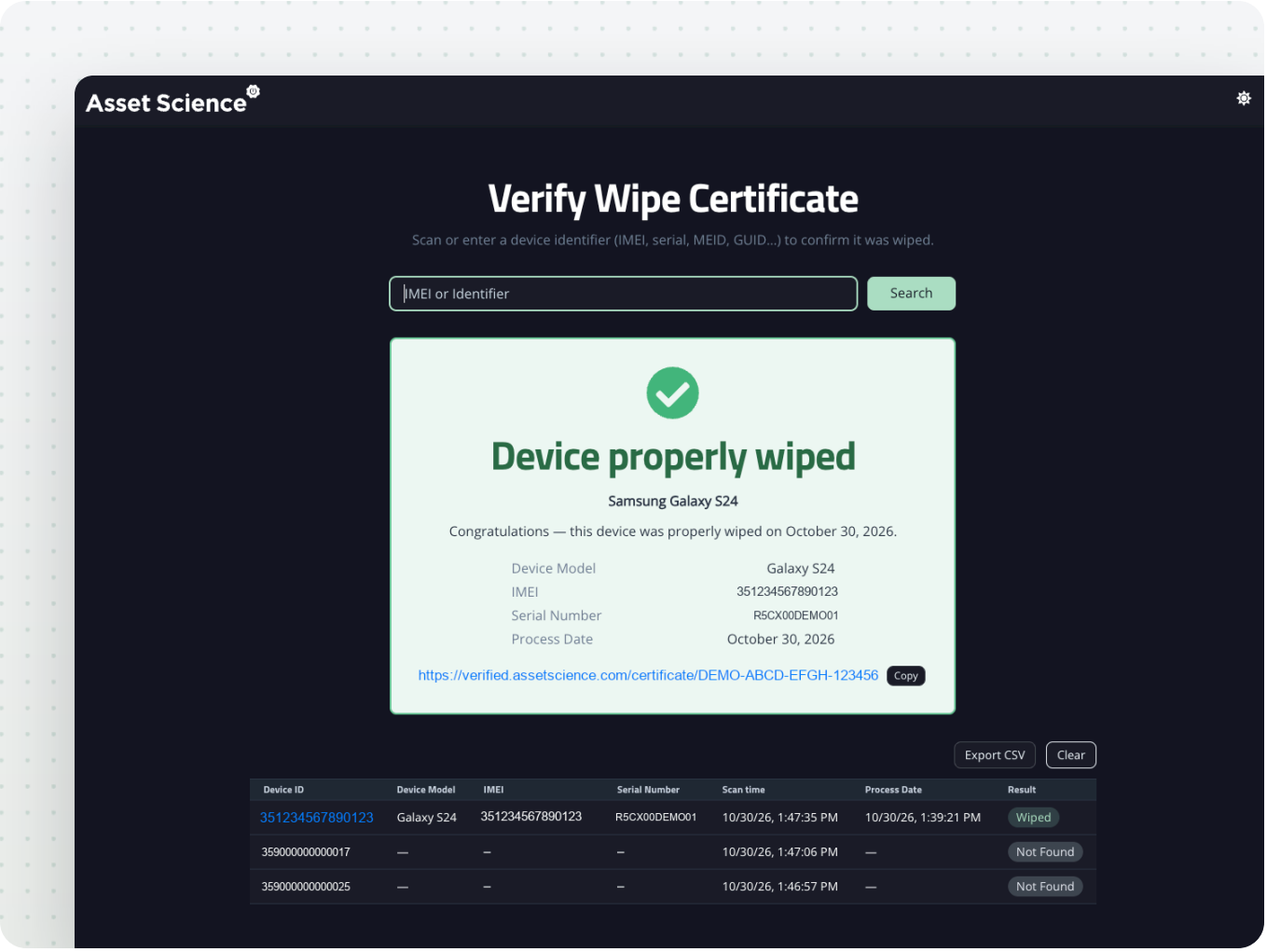
PUBLIC WEB CERTIFICATION

Der Nachweis verlässt Ihr Gebäude.

Wer eine IMEI oder Seriennummer hat, kann auf verified.assetscience.com nachsehen, was mit einem von Ihnen bearbeiteten Gerät geschah. Kein Konto, keine Anmeldung. Ein Lösch- und Diagnosezertifikat, ein teilbarer Link, ein PDF und Stapelexport für die Palette.



ZIELGRUPPE
Leiter Betrieb, Compliance & IT bei Geräteaufbereitern

ABFRAGE
IMEI · Seriennr. · MEID · GUID

ÖFFENTLICHE ZERTIFIKATE
verified.assetscience.com/verify

AUF EINEN BLICK

Die acht Fragen, die jeder Käufer stellt.

Dieses Produkt ist das Zertifikat, nicht die Prüfbank. Es veröffentlicht, was die Asset-Science-Plattform zu einem Gerät erfasst hat, für jeden, der dessen Kennung eintippen kann.

ZERTIFIKAT

● Ja

Öffentliche Web-Abfrage per IMEI, Seriennummer, MEID oder GUID auf verified.assetscience.com, ein teilbarer Zertifikatslink, ein PDF zum Download und Zertifikats-PDFs im Stapel.

ADISA-ZERTIFIZIERT

● AAL 4

Zertifikate aus **Pro-Diagnostics (PDD) und MacResto-re** tragen das Siegel ADISA-Sicherheitsstufe 4. Pro-Diagnostic PC ist nicht ADISA-zertifiziert; sein Lösch-bericht nennt stattdessen NIST-800-88-Methoden.

ART DER LÖSCHUNG

● NIST 800-88

Das Zertifikat nennt die **Methode der Inhaltslö-schung**: auf Geräten mit Volllaufwerksverschlüsse-lung wird der Schlüssel zerstört; auf unverschlüssel-ten Geräten wird überschrieben. Der Werksreset wird als Status-Kachel bestätigt.

GEFÜHRTE BEDIENERTESTS

● Nicht zutreffend

Getestet wird in den Diagnoseprodukten. Das Zertifi-kat **berichtet deren Ergebnisse**; es führt keine eige-nen Tests aus.

ART DER TESTS

● Berichtet, nicht ausgeführt

Diagnoseergebnisse mit Pass- und Fail-Zahlen, Akku-zustand und Gerätestatusprüfungen wie GSMA-Blacklist, Werksreset und eSIM, wie bei der Bearbei-tung erfasst.

HAUPTFUNKTIONEN

● 4

Öffentliche Abfrage ohne Konto. Teilbarer Link und PDF. **CSV-Stapelexport und Zertifikats-PDFs im Sta-pel.** Steuerung je Kunde, was veröffentlicht wird.

UNTERSTÜTZTE PLATTFORMEN

● Jeder Browser

Abfrage und Zertifikat sind **Webseiten**. Nichts zu in-stallieren, weder für Käufer noch Auditor noch Endbe-sitzer. Die Datensätze stammen aus der Asset-Sci-ence-Plattform.

DATENANALYSE UND API

● CSV

Gescannte Stapel lassen sich direkt aus der Abfrage-seite als CSV exportieren; die Massenabfrage nimmt eine CSV mit bis zu 30.000 Kennungen. Der zugrunde liegende Datensatz bleibt im Control Center mit vol-lem Datenexport.

1

Bearbeiten

Das Gerät wird auf der Plattform getestet und ge-löscht. Ein Datensatz je Gerät.

2

Veröffentlichen

Ihr Konto entscheidet, was öffentlich wird: Suche, Seite, PDF.

3

Abfragen

Jeder tippt oder scannt eine Kennung. Kein Konto nötig.

4

Prüfen

Das Zertifikat öffnet sich, mit Link zum Teilen und PDF zum Aufbewahren.

Ein Datensatz, drei Wege dorthin. Suche per Kennung auf der öffentlichen Seite, der teilbare Zertifikatslink oder der QR-Code auf dem Label. Alle drei führen zum selben Zertifikat für dieses Gerät.

WARUM EIN ÖFFENTLICHES ZERTIFIKAT ZÄHLT

Ein Datensatz, den außerhalb Ihres Gebäudes niemand lesen kann, ist eine Behauptung.

Jedes von Ihnen bearbeitete Gerät lässt sich per IMEI oder Seriennummer auf einer öffentlichen Seite abfragen: von Ihrem Käufer, vom Auditor Ihres Kunden oder von der Person, der das Telefon am Ende gehört.

DER KÄUFER

Öffnet den Nachweis aus der Datei, die Sie geschickt haben.

Zertifikatslinks reisen in exportierten Berichten mit. Wer ein Los erhält, glaubt nicht der Tabelle; jede Zeile zeigt auf eine Seite, die er selbst öffnen kann.

DER AUDITOR

Liest Vokabular, das er kennt.

Das Zertifikat nennt die Methode der Inhaltslöschung, zeigt GSMA-Blacklist- und Werksreset-Status und trägt das ADISA-Siegel, wo das bearbeitende Produkt es hält.

DER ENDBESITZER

Prüft das Telefon in seiner Hand.

Der QR-Code auf dem Label führt zum selben Zertifikat. Wer das Gerät am Ende hat, kann bestätigen, dass und wann es gelöscht wurde, ohne jemanden zu fragen.

Not Found heißt nicht gefunden. Ein Gerät, das niemand bearbeitet hat, kommt als Not Found zurück, nicht als beruhigende Leerstelle. Die Abfrage unterstellt nie eine Löschung, zu der kein Datensatz existiert.

ADISA

Zertifiziert nach ADISA-Sicherheitsstufe 4, im Umfang klar benannt.

Pro-Diagnostics und MacRestore sind nach ADISA-Sicherheitsstufe 4 zertifiziert, unabhängig geprüft vom ADISA Research Centre im Rahmen seines Product Claims Test. Die Zertifizierung gilt für die genannten Produkte. Pro-Diagnostic PC ist nicht zertifiziert, daher wird für Computer keine zertifizierte Löschung behauptet; seine Berichte nennen NIST-800-88-Methoden je Laufwerk.

NIST 800-88 REV. 2

Clear und Purge sind nicht austauschbar.

Jedes Laufwerk erhält die stärkere Methode, zu der es tatsächlich fähig ist, und die verwendete Methode steht im Löschbericht neben der Seriennummer dieses Laufwerks.

IEEE 2883

Die Terminologie des Standards selbst.

Terminologie der Sanitisierung und Erwartungen an die Verifikation folgen dem aktuellen Standard, sodass ein Auditor in unserem Bericht Vokabular liest, das er bereits kennt.

DIE ABFRAGE

Jeder kann ein Gerät prüfen, ohne Konto.

Scannen oder tippen Sie eine beliebige Kennung: IMEI, Seriennummer, MEID oder GUID. Das Ergebnis verlinkt direkt auf das Zertifikat dieses Geräts.

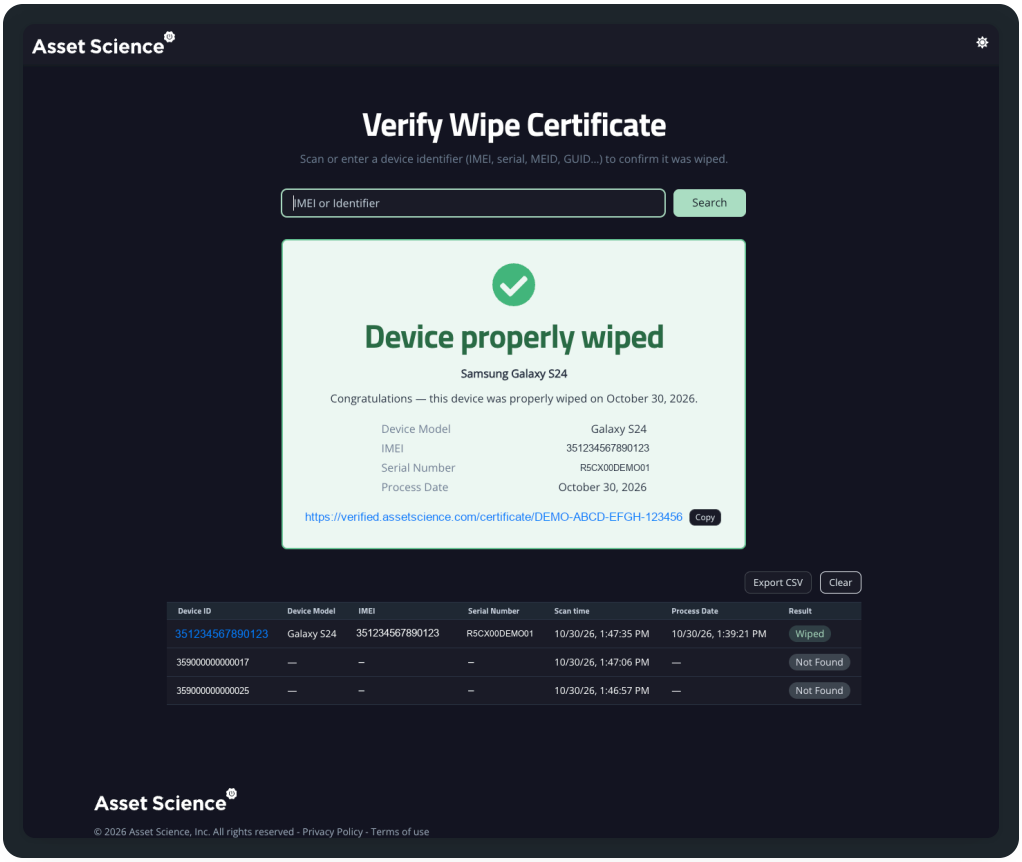


ABB. 1 verified.assetscience.com/verify. Ein gelöschtes Gerät liefert eine Ergebniskarte mit Modell, IMEI, Seriennummer und Bearbeitungsdatum sowie einen Zertifikatslink mit Copy-Button. Darunter der gescannte Stapel mit Export CSV. Zwei nie bearbeitete Kennungen kommen als Not Found zurück. Die gezeigten Kennungen sind synthetisch.

1

Scannen oder tippen

Ein Suchfeld. Barcode-Scanner oder Tastatur, jede unterstützte Kennung.

2

Ergebnis lesen

Gerät ordnungsgemäß gelöscht, mit Modell, IMEI, Seriennummer und Bearbeitungsdatum. Oder Not Found.

3

Link kopieren

Der Zertifikatslink öffnet sich für jeden, der ihn hat, sofern Ihr Konto das erlaubt.

4

Stapel exportieren

Jeder Scan der Sitzung landet in einer Tabelle. Export CSV nimmt den ganzen Stapel.

Nichts zu installieren, nichts zu registrieren. Die Seite steht jedem mit einer Kennung offen. Was er von einem Gerät sieht, das Sie bearbeitet haben, entscheiden die Veröffentlichungsschalter Ihres Kontos, beschrieben auf Seite 6.

DAS ZERTIFIKAT

Was gelöscht wurde, wie, und wie das Gerät getestet hat.

Die Seite hinter dem Ergebnis, von jedem mit dem Link als PDF herunterladbar. Ein Zertifikat je Gerät, mit eigener Zertifikats-ID.

KOPF UND ERGEBNIS

Zertifikats-ID, Sitzung, Modell, IMEI, Ergebnis.

Ein Banner nennt das Ergebnis in einer Zeile: Data Cleaning & Diagnostics Complete, Fully Functional. Reine Löschprozesse tragen stattdessen ein Data Cleaning Certificate, mit dem Banner Fully Wiped.

METHODE DER INHALTSLÖSCHUNG

Wie die Daten entfernt wurden, und das ADISA-Siegel.

Die Verschlüsselungsart wird bestimmt; auf volllaufwerksverschlüsselten Geräten wird der Schlüssel zerstört, auf unverschlüsselten wird überschrieben. Das Siegel ADISA-Sicherheitsstufe 4 steht unter dieser Aussage.

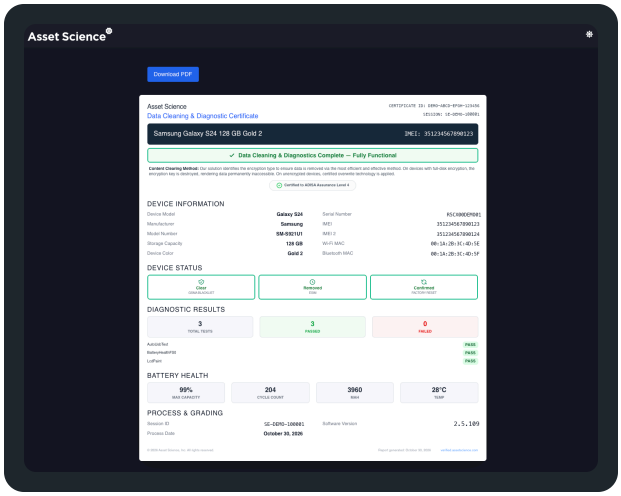


ABB. 2 verified.assetscience.com → Certificate. Ein Data Cleaning & Diagnostic Certificate mit dem Button Download PDF darüber. Kennungen, MAC-Adressen und Sitzungs-IDs sind synthetisch.

GERÄTEINFORMATIONEN

Zehn Identitätsfelder.

Gerätemodell · Hersteller · Modellnummer · Speicherkapazität · Gerätefarbe · Seriennummer · IMEI · IMEI 2 · Wi-Fi-MAC · Bluetooth-MAC

GERÄTESTATUS

Durchgeführte Prüfungen als Kacheln.

Grün, wenn eine Prüfung lief und bestand, rot, wenn sie lief und fehlschlug, bernstein N/A, wenn sie nicht lief. Geprüft werden unter anderem Aktivierung, Find My, GSMA-Blacklist, MDM, eSIM, Werksreset und Bauteile. Sperren werden gemeldet, nie entfernt.

DIAGNOSEERGEBNISSE UND AKKU

Zahlen, dann jeder Test mit Namen.

Gesamt, bestanden und fehlgeschlagen, dann jeder Test mit seinem PASS oder FAIL. Der Akkuzustand nennt maximale Kapazität, Ladezyklen, Kapazität in mAh und Temperatur.

PROZESS UND BEWERTUNG

Wer, wann, mit welcher Software.

Sitzungs-ID, Bearbeitungsdatum und die Softwareversion, die den Datensatz erzeugt hat. Die Fußzeile trägt das Erstellungsdatum und die Prüfadresse.

Das Zertifikat gibt die Aufzeichnung wieder, mehr nicht. Eine Prüfung, die nicht lief, zeigt N/A statt eines Bestehens. Ein Prozess, der vor dem Löschschritt scheiterte, zeigt Factory Reset als Failed, und das Banner lautet Process Failed. Ein fehlgeschlagenes Gerät wird nie stillschweigend zertifiziert.

SIE ENTSCHEIDEN, WAS ÖFFENTLICH IST

Drei Schalter je Kundenkonto, gesetzt im Control Center.

Die Veröffentlichung ist opt-in. Zertifikatsseite und PDF sind getrennte Schalter, sodass das Abschalten der Seite das PDF nicht von selbst privat macht. Das ist bewusst eine zweite Einstellung.

SCHALTER	WAS ER ERLAUBT
Ergebnisse in der öffentlichen Suche veröffentlichen	Jeder kann ein von Ihnen bearbeitetes Gerät per IMEI oder Seriennummer abfragen und dessen Lösch- und Diagnoseergebnisse sehen.
Öffentliche Zertifikatslinks erlauben	Wer einen Zertifikatslink hat, kann die Zertifikatsseite ohne Anmeldung öffnen. Steuert auch den Button Public Certificate in der Device History und die Zertifikatslinks in exportierten Berichten.
Öffentlichen PDF-Download erlauben	Wer einen Zertifikatslink hat, kann das Zertifikat ohne Anmeldung als PDF laden. Ein vom Schalter oben getrennter Schalter.

NACHWEISE IM STAPEL

Wer eine Palette abarbeitet, will Zertifikate nicht einzeln öffnen.

- **Gescannten Stapel als CSV exportieren** , direkt aus der Abfrageseite.
- **Massenabfrage von Geräten** aus einer CSV mit bis zu 30.000 Kennungen.
- **Zertifikats-PDFs im Stapel erzeugt und versendet**, nicht Gerät für Gerät.
- **Zertifikatslinks reisen in exportierten Berichten mit**, sodass ein Käufer den Nachweis aus der Datei öffnen kann, die Sie ihm schicken.

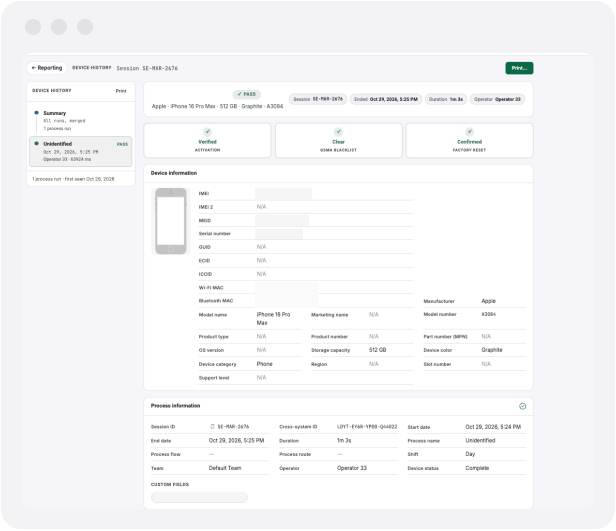


ABB. 3 Control Center → Device History. Dieselben Nachweise als Kacheln im Datensatz des Geräts: Aktivierung verifiziert, GSMA sauber, Werksreset bestätigt, über dem Kennungsblock und den Prozessinformationen. Die Kennungen sind synthetisch.

Innen und außen stimmen überein. Was das öffentliche Zertifikat zeigt, ist das, was die Device History im Control Center hält. Es gibt einen Datensatz je Gerät, und die öffentliche Seite ist eine Ansicht davon, keine zweite Kopie.

ÖFFENTLICHE VERIFIKATION

Zertifizierungsaussagen werden in diesem Markt routinemäßig über ihren Umfang hinaus gedehnt.

Unsere stehen in ihrem Umfang, mit den zertifizierten Produkten benannt. Und der Datensatz selbst ist öffentlich: Käufer, Auditor oder Endbesitzer können ihn lesen, ohne uns oder Ihnen glauben zu müssen.

Testen Sie die Abfrage an einem Gerät, das Sie bearbeitet haben.

Starten Sie eine kostenlose Testversion, bearbeiten Sie ein Gerät und fragen Sie es auf der öffentlichen Seite ab. Entscheiden Sie dann je Konto, was der Rest der Welt sehen darf.

KOSTENLOS TESTEN
onboarding.assetscience.com

ÖFFENTLICHE ZERTIFIKATE
verified.assetscience.com/verify

WEB
assetscience.com

© 2026 Asset Science. Screenshots stammen aus Produktions-Builds; gezeigte Gerätekennungen, Sitzungs-IDs, Bedienernamen und Kundendaten sind synthetisch. Produktnamen und Marken gehören ihren jeweiligen Eigentümern.