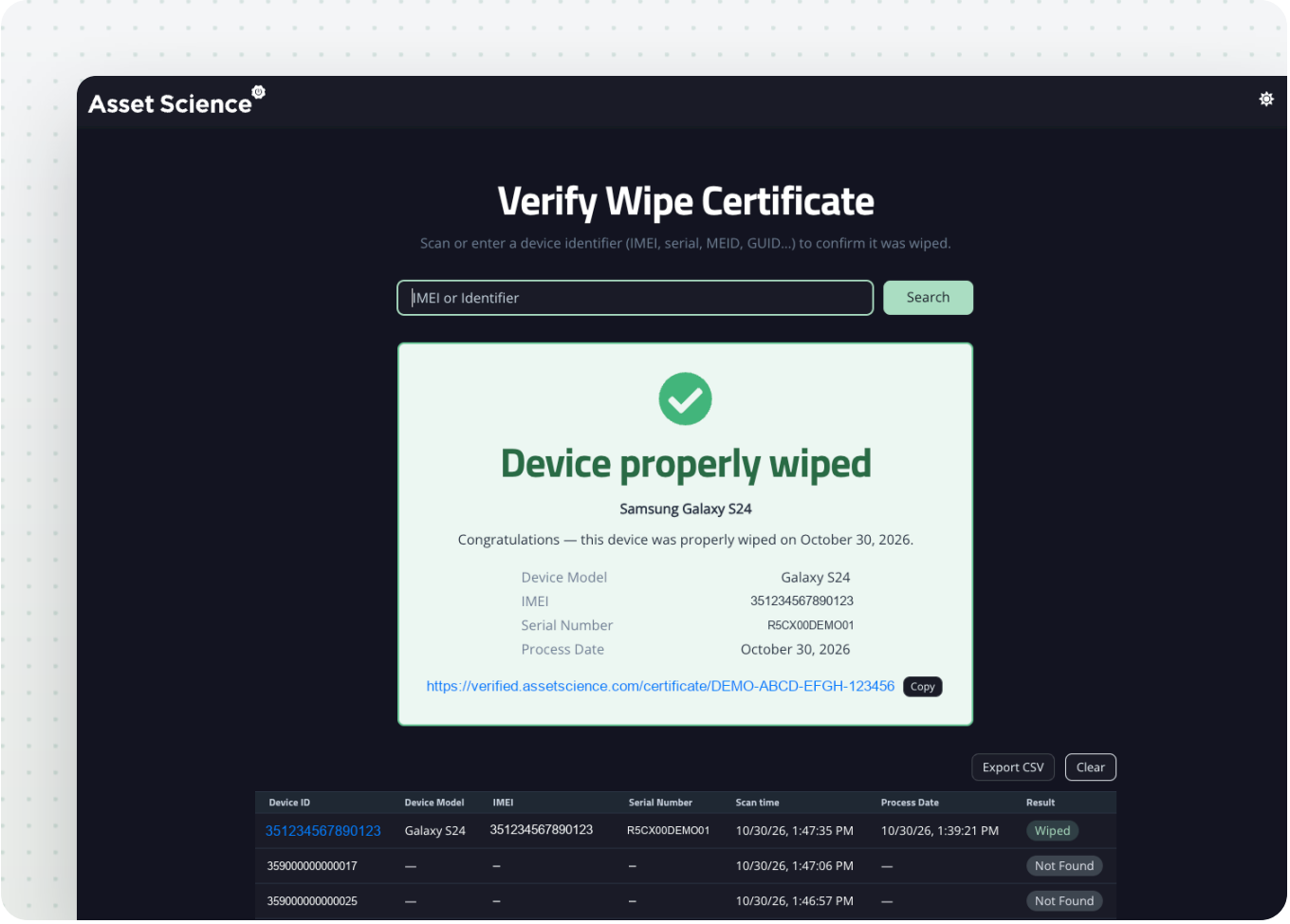
CERTIFICAZIONE WEB PUBBLICA

Le prove escono dal Vostro edificio.

Chiunque disponga di un IMEI o di un numero di serie può verificare che cosa è successo a un dispositivo elaborato da Voi su verified.assetscience.com. Nessun account, nessun accesso. Un certificato di cancellazione e diagnostica, un link condivisibile, un PDF e l'esportazione in blocco per il pallet.



DESTINATARI

Responsabili operations, compliance e IT dei processori di dispositivi

RICERCA

IMEI · Seriale · MEID · GUID

CERTIFICATI PUBBLICI

verified.assetscience.com/verify

IN SINTESI

Le otto domande che ogni acquirente pone.

Questo prodotto è il certificato, non il banco di test. Pubblica ciò che la piattaforma Asset Science ha registrato su un dispositivo, per chiunque sappia digitarne l'identificativo.

CERTIFICATO

● Sì

Ricerca web pubblica per IMEI, numero di serie, MEID o GUID su verified.assetscience.com, un link al certificato condivisibile, un PDF scaricabile e PDF dei certificati generati in blocco.

CERTIFICATO ADISA

● AAL 4

I certificati di **Pro-Diagnostics (PDD) e MacRestore** recano il marchio ADISA di livello di garanzia 4. Pro-Diagnostic PC non è certificato ADISA; il suo report di cancellazione indica invece i metodi NIST 800-88.

TIPO CANCELLAZIONE

● NIST 800-88

Il certificato indica il **metodo di cancellazione dei contenuti**: sui dispositivi con crittografia completa del disco la chiave viene distrutta; sui dispositivi non crittografati viene applicata la sovrascrittura. Il ripristino di fabbrica è confermato come riquadro di stato.

TEST GUIDATI DALL'UTENTE

● Non applicabile

I test avvengono nei prodotti diagnostici. Il certificato **ne riporta i risultati**; non esegue test propri.

TIPO DI TEST

● Riferiti, non eseguiti

Risultati diagnostici con conteggi di test superati e falliti, salute della batteria e controlli di stato del dispositivo come blacklist GSMA, ripristino di fabbrica ed eSIM, come registrati durante l'elaborazione.

FUNZIONI CHIAVE

● 4

Ricerca pubblica senza account. Link condivisibile e PDF. **Esportazione CSV in blocco e certificati PDF in blocco.** Controlli per cliente su ciò che viene pubblicato.

PIATTAFORME SUPPORTATE

● Ogni browser

La ricerca e il certificato sono **pagine web**. Nulla da installare per l'acquirente, l'auditor o il proprietario finale. I record provengono dalla piattaforma Asset Science.

ANALISI DEI DATI E API

● CSV

I lotti scansionati si esportano in CSV dalla schermata di ricerca; la ricerca in blocco accetta un CSV fino a 30,000 identificativi. Il record sottostante resta in Control Center con la sua esportazione dati completa.

1

Processo

Il dispositivo viene testato e cancellato sulla piattaforma. Un record per unità.

2

Pubblica

Il Vostro account decide cosa è pubblico: ricerca, pagina, PDF.

3

Ricerca

Chiunque digita o scansiona un identificativo. Nessun account.

4

Verifica

Si apre il certificato, con un link da condividere e un PDF da conservare.

Un record, tre modi per raggiungerlo. Cercare per identificativo sulla pagina pubblica, aprire il link condivisibile del certificato o scansionare il codice QR sull'etichetta. Tutti e tre portano allo stesso certificato per quel dispositivo.

PERCHÉ CONTA UN CERTIFICATO PUBBLICO

Un record che nessuno fuori dal Vostro edificio può leggere è solo un'affermazione.

Ogni dispositivo elaborato può essere cercato per IMEI o numero di serie su una pagina pubblica, dal Vostro acquirente, dall'auditor del Vostro cliente o da chi finisce per possedere il telefono.

L'ACQUIRENTE

Apre le prove dal file inviato.

I link ai certificati viaggiano dentro i report esportati. Un acquirente che riceve un lotto non si fida del foglio di calcolo; ogni riga punta a una pagina che può aprire da sé.

L'AUDITOR

Legge un lessico che già conosce.

Il certificato indica il metodo di cancellazione dei contenuti, mostra lo stato della blacklist GSMA e del ripristino di fabbrica e reca il marchio ADISA dove il prodotto di elaborazione lo possiede.

PROPRIETARIO FINALE

Controlla il telefono che ha in mano.

Il codice QR sull'etichetta porta allo stesso certificato. Chiunque finisca per avere il dispositivo può confermare che è stato cancellato, e quando, senza chiedere a nessuno.

Not Found significa non trovato. Un dispositivo che nessuno ha elaborato restituisce Not Found anziché uno spazio vuoto rassicurante. La ricerca non lascia mai intendere una cancellazione di cui non ha record.

ADISA

Certificato al livello di garanzia 4 ADISA, dichiarato nel suo ambito.

Pro-Diagnostics e MacRestore sono certificati al livello di garanzia 4 ADISA, testati in modo indipendente dall'ADISA Research Centre nell'ambito del suo Product Claims Test. La certificazione si applica ai prodotti indicati. Pro-Diagnostic PC non è certificato, quindi non viene formulata alcuna dichiarazione di cancellazione certificata per i computer; i suoi report indicano i metodi NIST 800-88 per ogni unità.

NIST 800-88 REV. 2

Clear e Purge non sono intercambiabili.

Ogni unità riceve il metodo più forte di cui è effettivamente capace, e il metodo usato è indicato nel report di cancellazione accanto al numero di serie di quell'unità.

IEEE 2883

La terminologia dello standard.

La terminologia di sanitizzazione e le aspettative di verifica sono allineate allo standard corrente, così un auditor che legge il nostro report legge un lessico che già conosce.

LA RICERCA

Chiunque può verificare un dispositivo, senza account.

Scansionare o digitare un identificativo qualsiasi: IMEI, numero di serie, MEID o GUID. Il risultato rimanda direttamente al certificato di quel dispositivo.

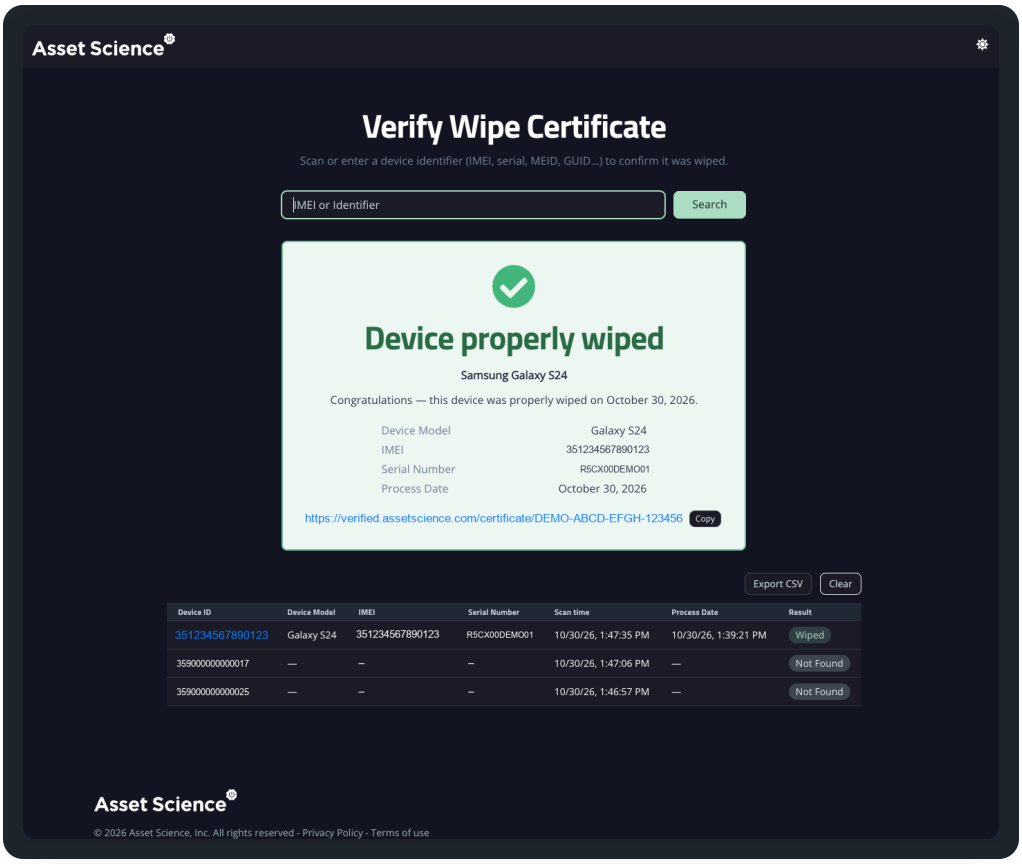


FIG. 1 verified.assetscience.com/verify. Un dispositivo cancellato restituisce una scheda risultato con modello, IMEI, numero di serie e data di elaborazione, e un link al certificato con un pulsante Copy. Sotto, il lotto scansionato con Export CSV. Due identificativi che nessuno ha elaborato restituiscono Not Found. Gli identificativi mostrati sono sintetici.

1

Scansionare o digitare

Un campo di ricerca. Scanner di codici a barre o tastiera, qualsiasi identificativo supportato.

2

Lettura del risultato

Dispositivo cancellato correttamente, con modello, IMEI, numero di serie e data di elaborazione. Oppure Not Found.

3

Copia del link

Il link al certificato si apre per chiunque lo possieda, se il Vostro account lo consente.

4

Export del lotto

Ogni scansione della sessione finisce in una tabella. Export CSV preleva l'intero lotto.

Nulla da installare, nessuna registrazione. La pagina è aperta a chiunque abbia un identificativo. Ciò che può vedere di un dispositivo elaborato da Voi è deciso dai controlli di pubblicazione del Vostro account, descritti a pagina 6.

IL CERTIFICATO

Che cosa è stato cancellato, come, e l'esito dei test del dispositivo.

La pagina dietro il risultato, scaricabile in PDF da chiunque abbia il link. Un certificato per dispositivo, con un proprio ID certificato.

INTESTAZIONE ED ESITO

ID certificato, sessione, modello, IMEI, esito.

Un banner dichiara l'esito in una riga: Data Cleaning & Diagnostics Complete, Fully Functional. I processi di sola cancellazione recano invece un Data Cleaning Certificate, con banner Fully Wiped.

METODO DI CANCELLAZIONE DEI CONTENUTI

Come i dati sono stati rimossi, e il marchio ADISA.

Il tipo di crittografia è identificato; sui dispositivi con crittografia completa del disco la chiave viene distrutta, su quelli non crittografati viene applicata la sovrascrittura. Il badge ADISA livello di garanzia 4 si trova sotto la dichiarazione.

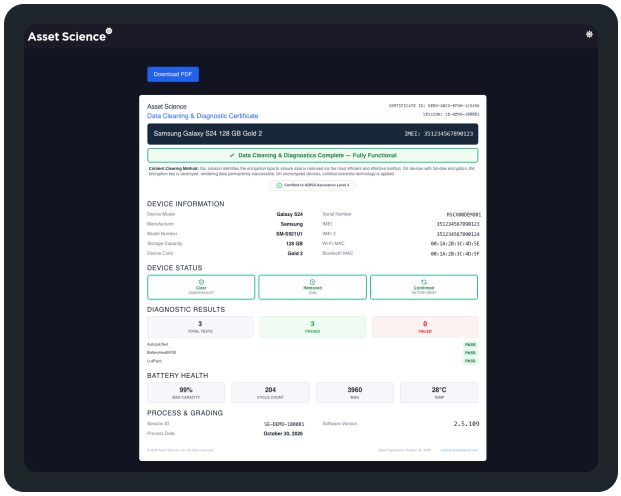


FIG. 2 verified.assetscience.com → Certificate. Un Data Cleaning & Diagnostic Certificate con il pulsante Download PDF sopra di esso. Identificativi, indirizzi MAC e ID di sessione sono sintetici.

DATI DEL DISPOSITIVO

Dieci campi d'identità.

Modello · Produttore · Numero modello · Capacità storage · Colore · Numero di serie · IMEI · IMEI 2 · Wi-Fi MAC · Bluetooth MAC

STATO DISPOSITIVO

Controlli eseguiti, in riquadri.

Verde quando un controllo è stato eseguito e superato, rosso quando è stato eseguito ed è fallito, ambra N/A quando non è stato eseguito. I controlli includono attivazione, Find My, blacklist GSMA, MDM, eSIM, ripristino di fabbrica e componenti. I blocchi sono segnalati, mai rimossi.

RISULTATI DIAGNOSTICI E BATTERIA

Conteggi, poi ogni test per nome.

Totale, superati e falliti, seguiti da ogni test con il suo PASS o FAIL. La salute della batteria riporta capacità massima, numero di cicli, capacità in mAh e temperatura.

PROCESSO E CLASSIFICAZIONE

Chi, quando, con quale software.

ID sessione, data di elaborazione e versione del software che ha prodotto il record. Il piè di pagina riporta la data di generazione e il sito di verifica.

Il certificato riflette la registrazione, nulla di più. Un controllo non eseguito mostra N/A anziché un esito positivo. Un processo fallito prima della fase di cancellazione mostra Factory Reset come Failed, e il banner riporta Process Failed. Un dispositivo fallito non viene mai certificato in silenzio.

DECIDETE VOI COSA È PUBBLICO

Tre interruttori per account cliente, impostati in Control Center.

La pubblicazione è opt-in. La pagina del certificato e il PDF sono interruttori distinti, quindi disattivare la pagina non rende di per sé privato il PDF. È un secondo controllo, deliberatamente.

CONTROLLO	COSA CONSENTE
Risultati nella ricerca pubblica	Chiunque può cercare un dispositivo elaborato da Voi per IMEI o numero di serie e vederne i risultati di cancellazione dati e diagnostica.
Link pubblici al certificato	Chiunque abbia un link al certificato può aprire la pagina del certificato senza accedere. Controlla anche il pulsante Public Certificate in Device History e i link ai certificati nei report esportati.
Download PDF pubblico	Chiunque abbia un link al certificato può scaricare il certificato in PDF senza accedere. Un interruttore distinto da quello della pagina sopra.

PROVE A LOTTI

Chi cancella un pallet non vuole aprire un certificato alla volta.

- **Export in CSV di un lotto scansionato** direttamente dalla schermata di ricerca.
- **Ricerca in blocco** da un CSV fino a 30,000 identificativi.
- **PDF dei certificati generati e inviati in blocco**, non un dispositivo alla volta.
- **I link ai certificati viaggiano nei report esportati**, così un acquirente può aprire le prove dal file che gli inviate.

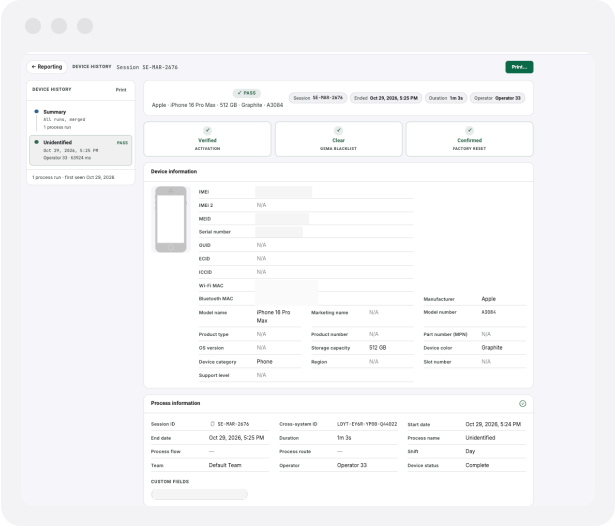


FIG. 3 Control Center → Device History. Le stesse prove come riquadri sul record del dispositivo: attivazione verificata, GSMA libero, ripristino di fabbrica confermato, sopra il blocco identificativi e le informazioni di processo. Gli identificativi sono sintetici.

Dentro e fuori coincidono. Ciò che mostra il certificato pubblico è ciò che Device History contiene in Control Center. C'è un record per dispositivo, e la pagina pubblica ne è una vista, non una seconda copia.

VERIFICA PUBBLICA

In questo mercato le dichiarazioni di certificazione vengono abitualmente estese oltre il loro ambito.

Le nostre sono dichiarate nel loro ambito, con i prodotti certificati indicati. E il record stesso è pubblico: un acquirente, un auditor o un proprietario finale può leggerlo senza credere sulla parola a noi, o a Voi.

Provate la ricerca su un dispositivo elaborato da Voi.

Avviate una prova gratuita, elaborate un dispositivo e cercatelo sulla pagina pubblica. Poi decidete, per account, che cosa il resto del mondo può vedere.

PROVA GRATUITA
onboarding.assetscience.com

CERTIFICATI PUBBLICI
verified.assetscience.com/verify

WEB
assetscience.com

© 2026 Asset Science. Le schermate provengono da build di produzione; identificativi dei dispositivi, ID di sessione, nomi degli operatori e dati dei clienti mostrati sono sintetici. I nomi e i marchi dei prodotti appartengono ai rispettivi proprietari.