



DATENBLATT · DATEN-APIS · DEVICE FINGERPRINT

Dasselbe Gerät, neues Konto? Ab jetzt erkennen Sie das Gerät wieder.

Device Fingerprint erkennt Browser und Geräte über ein Browser-SDK wieder und liefert je Gerät eine stabile visitor_id, Erst- und Letztkontakt, Risikofaktoren und ein Bot-Signal. Für Anmeldung, Checkout und Kontoschutz: per SDK, REST-API und MCP.

AUF EINEN BLICK

Eine visitor_id je Gerät, je Organisation getrennt gespeichert. Beim nächsten Login prüft /fingerprint/verify, ob es dasselbe Gerät ist, und zeigt, welche Signale passen.

01 · WURUM ES GEHT

Neue E-Mail, neues Konto? Das Gerät bleibt dasselbe.

Wer mehrere Konten anlegt oder fremde Zugangsdaten nutzt, wechselt E-Mail und Namen, das Gerät aber selten. Device Fingerprint gibt jedem Browser eine stabile Kennung und meldet, wann er zuerst und zuletzt da war und was an der Sitzung auffällt.

SIGNALE

Canvas, WebGL, Audio, Schriften, Hardware und Bildschirm per SDK, dazu IP und User-Agent

ERGEBNIS

visitor_id, Besuche, Erst- und Letztkontakt, Gerät, Risiko 0–100 mit Faktoren, Bot-Signal

ZUGANG

Browser-SDK mit Publishable Key, REST-API /fingerprint, MCP im Katalog /mcp-full

DATENSCHUTZ

Gerätedaten je Organisation getrennt, Löschung je Kennung mit POST /privacy/forget

**Stabile Kennung**

Das SDK bildet Hashes aus Canvas, WebGL, Audio und Schriften. Bringt ein Browser eine neue ID mit, aber gleiche Werte, läuft seine Historie weiter.

Verifizieren beim Login

/fingerprint/verify vergleicht JA4, User-Agent, IP, Canvas und WebGL mit dem gespeicherten Gerät und liefert verified und matchScore.

Risiko mit Gründen

risk.factors nennt, was auffällt: VPN, Proxy, Tor, Rechenzentrum, Relay, eine unmögliche Reisegeschwindigkeit oder ein bekannter Bot.

Bot-Erkennung

bot liefert is_bot, Score und Signale, serverseitig berechnet: Headless-Browser, Automatisierung, Software-Rendering, fehlende Interaktion.

Ähnliche Geräte

/fingerprint/similar findet Geräte mit ähnlichen Hashes in Ihrem Bestand, mit Ähnlichkeit in Prozent und einstellbarer Schwelle.

Geräte im selben Netz

/fingerprint/linked zeigt, welche anderen Geräte aus denselben Netzen kamen, etwa mehrere Geräte aus einem Haushalt oder Büro.

02 · SO FUNKTIONIERT ES

SDK einbinden, Kennung holen. Beim Login vergleichen.

Das SDK läuft auf Ihrer Website und spricht mit einem Publishable Key direkt mit der API. Ihr Backend vergleicht später mit dem API-Schlüssel.

1

Publishable Key anlegen

Unter **API & Entwickler** > **API-Keys** wählen Sie **Neuen Key erstellen**, dann den Typ **Veröffentlichter Schlüssel**, und tragen die Domains Ihrer Website ein.

2

SDK einbinden

Laden Sie `/fingerprint/sdk` per Script-Tag und rufen Sie `PaperOfficeFingerprint.load` mit Ihrem Schlüssel und danach `get()` auf.

3

Kennung speichern

Das Ergebnis enthält die `visitor_id`. Speichern Sie sie in Ihrem System zu Login oder Bestellung.

4

Vergleichen und auswerten

Beim nächsten Login prüft `POST /fingerprint/verify` das Gerät. `risk.factors` und `bot` zeigen, was auffällt.

TECHNISCHE DATEN

MERKMAL	DETAILS
SDK	<code>https://api.paperoffice.ai/latest/fingerprint/sdk</code> , als ES-Modul unter <code>/fingerprint/sdk.esm</code>
Endpunkte	<code>POST /fingerprint/identify</code> , <code>POST /fingerprint/verify</code> , <code>GET /fingerprint/device</code> , <code>/similar</code> , <code>/linked</code>
Antwortfelder	<code>visitor_id</code> , <code>visits</code> , <code>first_seen</code> , <code>last_seen</code> , <code>device</code> , <code>ip</code> , <code>risk (score, level, factors)</code> , <code>bot</code>
Zugang	Browser: Publishable Key (<code>po_pk_</code>); Backend: API-Schlüssel; MCP im Katalog <code>/mcp-full</code>
Löschung	<code>POST /privacy/forget</code> mit <code>visitor_id</code> oder <code>identifier_hash</code> ; Antwort mit <code>tombstone</code>
Mandantentrennung	Gerätedaten werden je Organisation getrennt gespeichert und abgefragt
Abrechnung	Nach Verbrauch

03 · IM EINSATZ

Wo das Gerät zählt. Drei typische Abläufe.

Login absichern

Meldet sich ein bekanntes Konto von einem fremden Gerät oder mit unmöglicher Reisegeschwindigkeit an, fragt Ihre Anwendung einen zweiten Faktor ab.

Mehrfachanmeldungen sehen

Legt dasselbe Gerät neue Konten an, steht in Ihrem System dieselbe visitor_id an mehreren Konten. /fingerprint/linked zeigt dazu Geräte aus demselben Netz.

Bots von Menschen trennen

Bei Registrierung oder Gutscheinaktion hält Ihre Anwendung Sitzungen mit bot.is_bot zurück, etwa Headless-Browser oder Automatisierung ohne Interaktion.

HÄUFIGE FRAGEN

Welche Signale nutzt das SDK?

Canvas, WebGL, Audio, Schriften, Hardware- und Bildschirmmerkmale sowie Maus-, Tastatur- und Touch-Muster für die Bot-Erkennung. Serverseitig kommen IP und User-Agent dazu.

Wie gehe ich mit Löschanfragen um?

POST /privacy/forget löscht Geräteprofil, Verknüpfungen, Verlauf und Warnungen zur Kennung in Ihrer Organisation. Ein Sperrvermerk verhindert, dass dieselbe Kennung erneut erfasst wird.

Wie erkenne ich ein bekanntes Gerät?

identify meldet is_new und visits. GET /fingerprint/device liefert zu einer visitor_id Erst- und Letztkontakt, Besuche, Browser, Plattform und Land.

Wer ist für die Daten verantwortlich?

Sie als Verantwortlicher legen Zweck und Rechtsgrundlage fest. Die Antwort von identify nennt im Block compliance Datenkategorien, Zwecke und die empfohlene Rechtsgrundlage.

JETZT STARTEN

Geräte wiedererkennen, ab dem nächsten Login

Konto anlegen, unter **API & Entwickler > API-Keys** einen Publishable Key für Ihre Domain erstellen und das SDK auf Ihrer Anmeldeseite einbinden.

paperoffice.ai/de/ki-device-fingerprint-geraete-fingerprint-browser-tracking-fraud-prevention



MEHR ZUM MODUL

paperoffice.ai/de/ki-device-fingerprint-geraete-fingerprint-browser-tracking-fraud-prevention

PREISE

paperoffice.ai/de/preise

KONTAKT

paperoffice.ai/de/kontakt