Auf Sicherheit getrimmt: GrapheneOS

(Folge 3 in der Android-Reihe)

Matthias Brüstle

Nürnberg 2025-11-23

Aus Folge 1 2011

„ohne“ Google?

- Einfaches Flashen neuer Software auf das Galaxy S II
- 13. September 2011: Modifiziertes Original-ROM installiert – Lite'ning - „root“
- 20. September 2011: Android Open Source Project (AOSP) ROM installiert – Cyanogen Mod 7
- Google Closed Source separat zu installieren: Market, Talk, Vending, Backup, Maps

...oder auch **nicht**

Halb aus Folge 2 2019

Seitdem

- Aus Cyanogen Mod 7 wurde LineageOS
- Aus dem Samsung SII wurde Samsung S5

- Daraus ein S9
- Dann hatte der Akku schon wieder Blähungen
- Und nun? So ohne Daumenverlängerung?
- Ein technik-affiner Freund meinte: Probier doch GrapheneOS aus
- Und jetzt bin ich hier mit einem Pixel 7a

Glücklicherweise ohne Daumenverlängerung

- 2014: https://androidmag.de/news/technik-news/japanischer-hersteller-fertigt-daumen-verlangerungen-fur-grose-phablets/

GrapheneOS (GOS)

- https://de.wikipedia.org/wiki/GrapheneOS "GrapheneOS ist ein [Android-]Open-Source-Betriebssystem für Google-Pixel-Geräte, das speziell auf Datenschutz und Sicherheit ausgerichtet ist."
- ...und auch deutlich auf Anwenderfreundlichkeit
- Wobei sich selbstverständlich die Ziele ein kleines Bisschen beissen

Datenschutz & Sicherheit: Was sagen andere dazu?

- https://www.kuketz-blog.de/grapheneos-der-goldstandard-unter-den-android-roms-custom-roms-teil7/
  "GrapheneOS setzt Standards in puncto Sicherheit und Datenschutz, die von keinem anderen Android-System erreicht werden."

- https://www.androidauthority.com/cellebrite-leak-google-pixel-grapheneos-security-3611794/
  "A leaked Cellebrite chart shows Pixel phones running GrapheneOS largely resist the company's forensic unlocking tools."

Table 3: Android OS Access Support Matrix – Google Pixel 7.69.1

Model / State	Standard Android OS, BFU	Standard Android OS, AFU	Standard Android OS, Unlocked	GrapheneOS, BFU *	GrapheneOS, AFU *	GrapheneOS, Unlocked
Pixel 6 / Pixel 6 Pro / Pixel 6a	BFU Yes BF No	FFS Yes BF No	FFS Yes	BFU Yes, up to late 2022 SPL BF No	FFS Yes, up to late 2022 SPL BF No	FFS Yes
Pixel 7 / Pixel 7 Pro / Pixel 7a / Pixel Tablet / Pixel Fold	BFU Yes BF No	FFS Yes BF No	FFS Yes	BFU Yes, up to late 2022 SPL BF No	FFS Yes, up to late 2022 SPL BF No	FFS Yes
Pixel 8 / Pixel 8 Pro	BFU Yes BF No	FFS Yes BF No	FFS Yes	BFU Yes, up to late 2022 SPL BF No	FFS Yes, up to late 2022 SPL BF No	FFS Yes

Datenschutz & Sicherheit: Was sagen andere dazu? (2)

- https://piunikaweb.com/2025/11/21/grapheneos-criminals-choice-in-france-after-police-fail-to-crack-google-pixel/
  "During a raid, investigators seized a Google Pixel running GrapheneOS. However, when police IT specialists attempted to access the device’s contents, the phone reportedly “mysteriously reset,” wiping potential evidence."
- https://en.wikipedia.org/wiki/Operation_Trojan_Shield
  https://darknetdiaries.com/transcript/146/
  Wobei die Polizei selbst Händys Kriminellen gibt, die möglicherweise auf GrapheneOS basieren

Anwenderfreundlichkeit: Anleitungen

- Meine Erfahrung mit "Custom ROMs"/alternativen Android-Betriebssystemen:
  - Verschiedene Informationsquellen
  - Für verschiedene Software-Stände
  - Kurz: Anleitungsdschungel
- Hier eine zentrale und klare Informationsquelle: https://grapheneos.org
- Installation, Features, technische Beschreibung, FAQ
- Leider nur auf Englisch (AFAIK)

Anwenderfreundlichkeit: Installation per Web Installer

1) Eine, offizielle Anleitung:
   https://grapheneos.org/install/web (nur Englisch) für Chrome und Edge
2) OEM Unlocking (etwas affiges Rumgedrücke in den Android-Settings)
3) Bootloader starten (Volume Down-Taste beim Booten)
4) Händy mit USB-Kabel am PC anschließen
   (Linux: Benutzerrechte, ggf. fwupd aus)
5) Bootloader entsperren (1. Button auf der Webseite)
6) Graphene-Dateien herunterladen (2. Button auf der Webseite)
7) Graphene übertragen (3. Button auf der Webseite)
8) Bootloader sperren (4. Button auf der Webseite)
9) GrapheneOS booten
10) OEM Unlocking ausschalten (im initialen Setup angeboten)

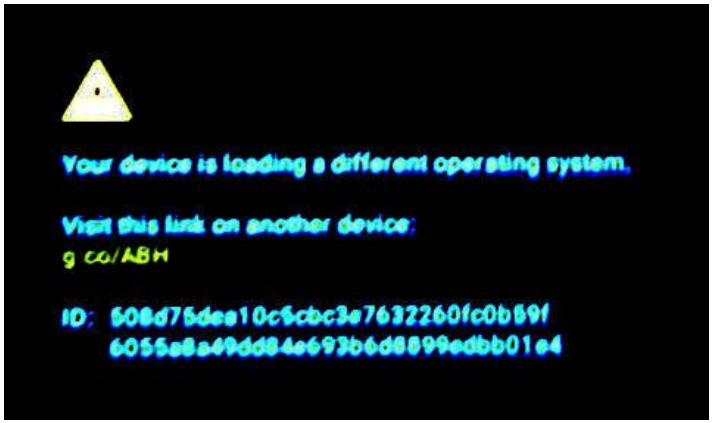
Anwenderfreundlichkeit: Installation per Web Installer

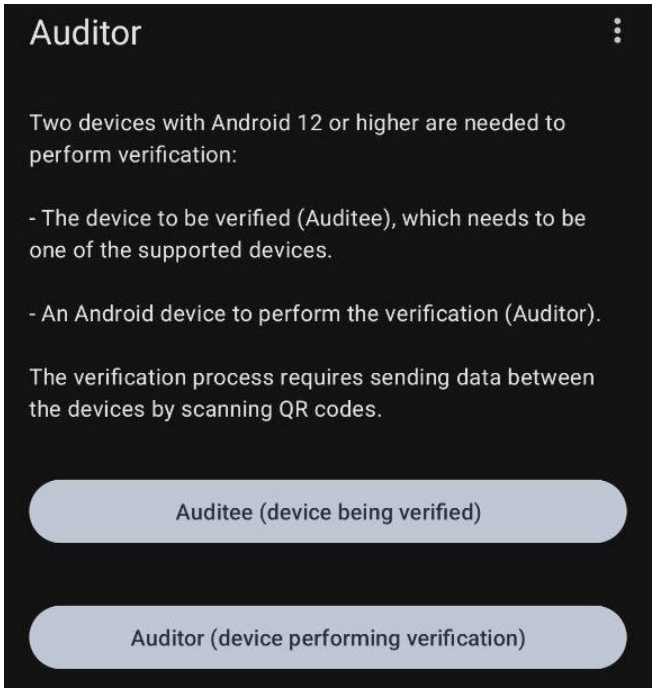
11) GrapheneOS mit Secure Boot genießen
(Boot Key Hash prüfen, wohnlich einrichten)

von Harry Whittier Frees

Datenschutz & Sicherheit: Secure Boot & Attestation

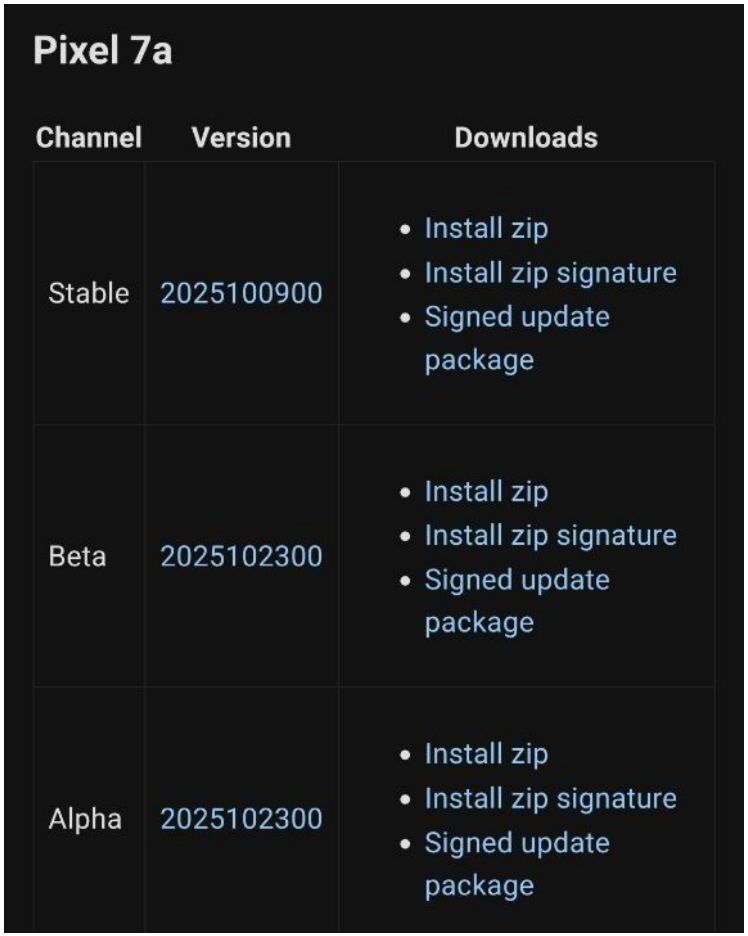
- Secure Boot
- Im Gegensatz zu den meisten(?) AOSP-Projekten
- Boot Key Hash prüfen wie in der Installationsanleitung
- Attestation-App und -Web-Service
- https://attestation.app/tutorial





Anwenderfreundlichkeit: Updates

- Automagisches Herunterladen/Prüfen/Vorbereiten
- Nur noch rebooten wenn es passt
- Genau so beim Updaten auf neue Android-Version (14 -> 15 -> 16)
- "Huch! War das nicht neulich noch 14?"
- Release Channel: Testing / Alpha / Beta / Stable

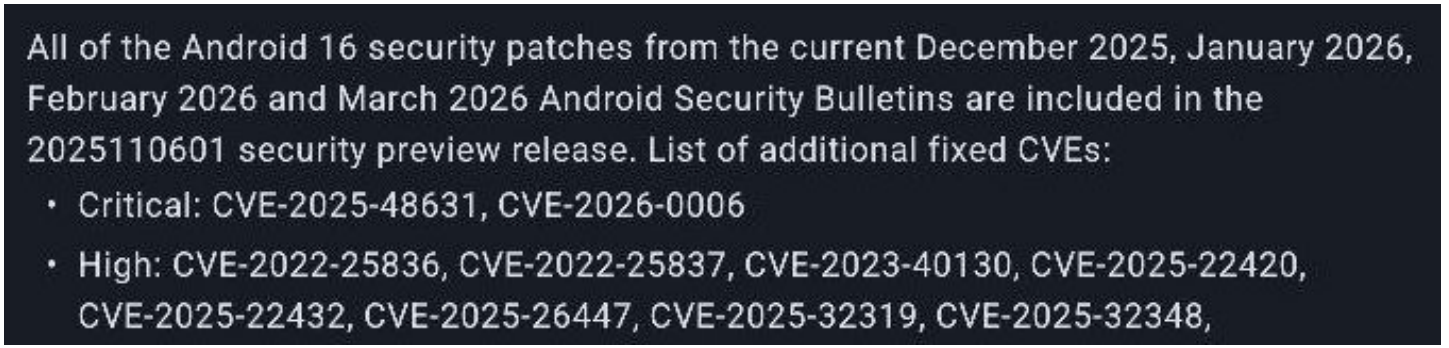


Pixel 7a

Channel	Version	Downloads
Stable	2025100900	• Install zip • Install zip signature • Signed update package
Beta	2025102300	• Install zip • Install zip signature • Signed update package
Alpha	2025102300	• Install zip • Install zip signature • Signed update package

Datenschutz & Sicherheit: Patches

- Aktuellster verfügbarer Patch-Stand
- Patches werden möglichst schnell ausgerollt
- Updates auch zwischendurch, z.B. Teilupdates
- Neu: Binäre Android-Patches der Zukunft



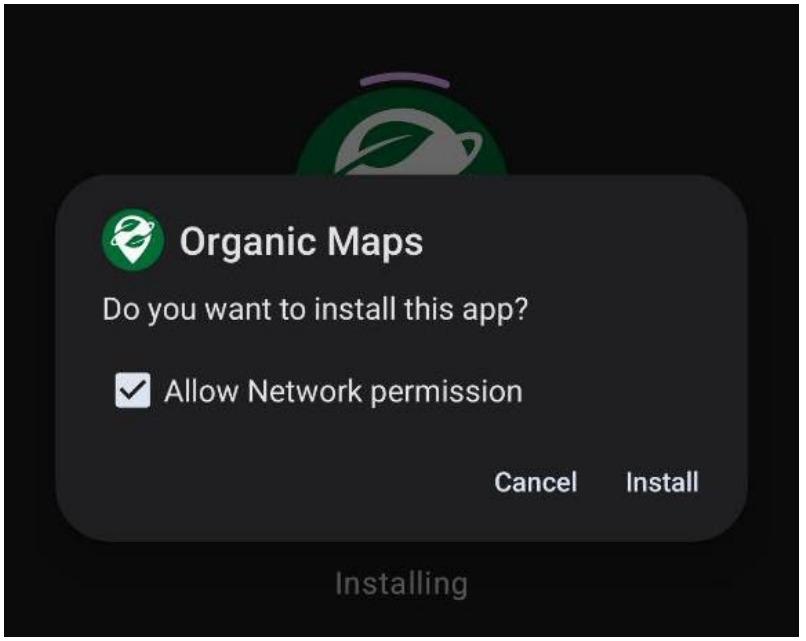
- Erwartet vom Hersteller mindestens 5 Jahre zeitnahe Hardware-Patches

Datenschutz & Sicherheit: Hardware

- 26 Anforderungen an die Hardware: https://grapheneos.org/faq#future-devices
- Unterstützt:
  - Pixel 9a, 9 Pro Fold, 9 Pro XL, 9 Pro, 9
  - Pixel 8a, 8 Pro, 8
  - Pixel Fold
  - Pixel Tablet
  - Pixel 7a, 7 Pro, 7
  - Pixel 6a, 6 Pro, 6
- **Eingeschränkte Auswahl kann Ausschlusskriterium sein**
- Graphene-Händy von großen Hersteller für 2026/27 angekündigt

Datenschutz & Sicherheit: to root or not to root

- Apps mit root können weiterte Funktionen umsetzen, z.B. Firewall, aber auch ein Sicherheitsproblem sein
- Rooting von GrapheneOS nicht unterstützt
- Ich hab es aber auch nicht vermisst
- App-Permission: Netzwerkzugriff über alle Wege gefiltert (besser als AFWall+)
- Viel/alle In-App-Werbung einfach so weg (AdAway nicht nötig)



Datenschutz & Sicherheit
Daten/App-Abteilungen

- Mehrere Benutzer
  - z.B. für verschiedene Händynutzer
- Work Profile (Arbeitsprofil)
  - benötigt App zur Verwaltung (z.B. Island)
- Private Space (Vertrauliches Profil)
  - Seit Android 15
  - Verwaltung per Einstellungen
  - Ich sehe keinen grundlegenden Unterschied
  - Würde bei Neueinrichtung das nehmen

Datenschutz & Sicherheit: Google-Apps

- Google Play, Android Auto und Google Services laufen in einer Sandbox
- Wie jede normale App ohne spezielle Rechte und Privilegien
- Umleitung von Diensten auf GrapheneOS-Dienste, z.B. Ortungsdienste (abschaltbar)
- Gezielt in Profilen installierbar, da wie normale App

Datenschutz & Sicherheit: Appstores mit und ohne Google

https://www.youtube.com/watch?v=IAoCfrqxIEg

1) GrapheneOS App Store (12 Apps: System Apps, Accrescent, Groogle Play Store)
2) Accrescent (36 Apps, soll mehr werden)
3) Obtainium (+AppVerifyer) (App-Installer fuer Releases von Entwicklern auf github) – finde ich umständlich
4) Google Play Store (persönliches Konto) und/oder Aurora (anonymes Konto)
5) f-droid, besser Neo Store mit alternativen Repositories, e.g. IzzyOnDroid, GuardianProject.

https://privsec.dev/posts/android/f-droid-security-issues/

Datenschutz & Sicherheit: Ein paar (nützliche) Beispiele aus einer langen Liste

- https://grapheneos.org/features
- "GrapheneOS is heavily focused on protecting users against attackers exploting unknown (0 day) vulnerabilities."
- Ganz viel "härten" von Betriebssystem- und App-Komponenten, z.B. zuverlässiges Löschen von ungenutztem Speicher, Vergrößerung des Adressbereichs für zufällige Adressen, Sandboxing
- Folgende Feature-Liste enthält nur GrapheneOS-spezifische Erweiterungen

Datenschutz & Sicherheit: Auto reboot

- "the phone reportedly “mysteriously reset”"
- Grundeinstellung:
  18 Stunden nach der Bildschirmsperre bootet das Händy
  => BFU mit komplet gesperrter Dateisystemverschlüsselung
- Einstellbar auf 10 Minuten bis 72 Stunden
- Im init-Prozess implementiert
- Absturz des init-Prozesses
  => Kernel Panic
  => Reboot

Datenschutz & Sicherheit:
Reduzierung der angreifbaren Oberfläche

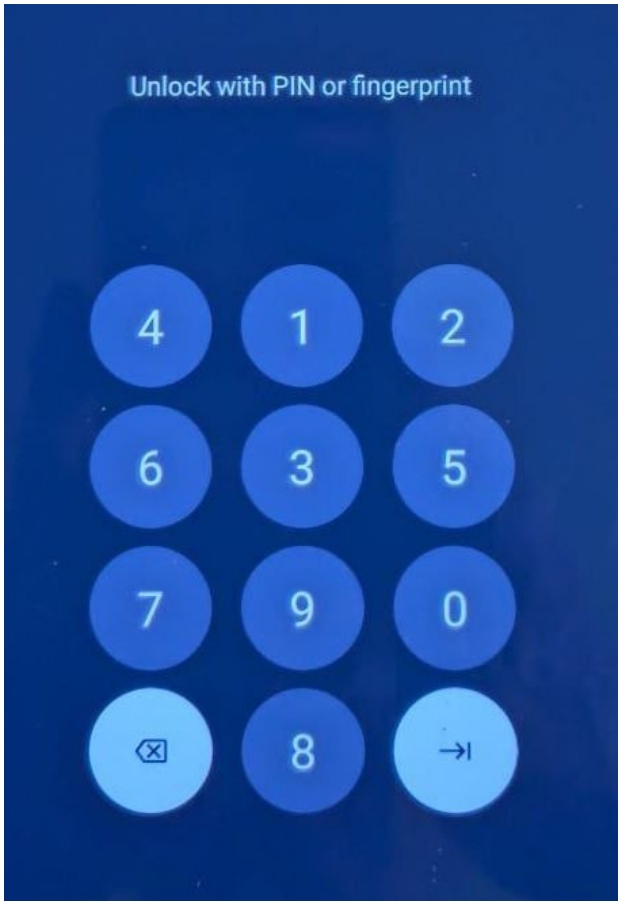
- Deaktivieren unbenutzten Codes
- Optionale Features standardmäßig abschalten
- WiFi und Bluetooth mit Timer abschaltbar
- USB konfigurierbar
  aus / an / nur Laden / nur Laden wenn gesperrt
- USB-Blockierung via USB-Controller und GrapheneOS-Kernel

Datenschutz & Sicherheit: Storage Scopes / Contact Scopes

- Bei Scopes denkt die App sie hat Zugriff auf alles
- Sie bekommt aber nur die Dateien bzw. Kontakte, die man für diese App freischaltet
- Z.B wenn man in einer Messenger-App Zugriff auf die Kontakte braucht um jemandem neu schreiben zu können
- Oder bei Wero (dazu mehr bei den Lightning Talks – Cliffhanger :-))

Datenschutz & Sicherheit: erweiterte PIN-Funktionen

- PIN Scrambling
- Fingerabdruck mit einem Fehlbedienungszähler von 5
- 2-Faktor-Authentisierung: PIN + Fingerabdruck
- Max. Passwortlänge 128-Zeichen (fließt in den Schlüssel für die Dateisystem-verschlüsselung ein)
- ab 140 PIN-Versuchen Verzögerungen von 1 Tag (durch das Sicherheitsmodul) => 6 Ziffern sind eigentlich ausreichend
- Notfall-PIN zum Zurücksetzen des Händys



Datenschutz & Sicherheit: Schließen von VPN-Schlupflöchern

- verhindert DNS-Anfragen am Virtual Private Network (VPN) vorbei auch in Ausnahmefällen, z.B. bei VPN-Verbindungsprobleme
- verhindert Multicast-Pakete abseits des VPN
- getrennte VPN-Profile für andere Benutzer, Arbeitsprofile und Vertrauliche Profile
- verhindert parallele Kommunikation über Systemaufrufe
- und noch ein paar andere Fixes

Datenschutz & Sicherheit: Weiter Mechanismen für Datenschutz

- Per default nur Verbindungen zu Graphene-Servern, z.B. Zeitserver, Ortungsdienst
- Der Netzwerkortungsdienst (über sichtbare WiFis) frägt beim Server die WiFi-Postionen ab und bestimmt selbst den Standort (im Ggs. zur Standortbestimmung durch den Server)
  Eine Offline-Datenbank in Planung
- MAC Address Randomization (bei jedem Verbindungsaufbau neu)
- Apps und Graphene-Services bekommen keine Händy-ID

Memory Tagging

- Seit November 2023 ab Pixel 8 verfügbar
- Hardware-Support nötig
- Schützt frisch installiert Kernel, alle OS-Prozesse, alle GrapheneOS-Apps, andere Apps, die kompatibel sind
- Kann für alle Apps eingeschalten werden
- Deutlich mehr abgesicherter Code als bei anderen Systemen, z.B. jetzt neu bei iPhone (Memory Integrity Enforcement)

Was ist (noch) nicht so gut?

- Backup:
  Seedvault ist eine Notlösung mit der niemand zufrieden ist
  Ganz neue Backup-Lösung geplant
  Ohne root auch keine App-Lösung
- Webbrowser:
  Vanadium ist ein gehärteter Chrome, aber (noch) ohne AdBlocker
  Ich möchte eigentlich Chrome-Monokultur vermeiden
- Google Pay:
  Technische Sicherheitsanforderungen übererfüllt
  Geht aber nicht, weil kein Google-Zertifikat (Play Integrity API)
  Einige wenige Bank-Apps gehe auch nicht
  https://privsec.dev/posts/android/banking-applications-compatibility-with-grapheneos/

Anwenderfreundlichkeit vs. Datenschutz & Sicherheit

- Anwenderfreundlichkeit priorisierbar
- Trotzdem noch viele Vorteile bei Datenschutz & Sicherheit
- Kaum komplizierter als die normale Android-Installation, wenn nicht gewollt, z.B.
  - App-Store-Wahl, man muss zumindest Google Play nachinstallieren
  - Umfangreichere Einstellungsmenüs
- Ich bin seitdem ich diesen Vortrag erstellt habe noch mehr von GrapheneOS überzeugt

Links

- Anleitung für den Web-Installer
  https://grapheneos.org/install/web
- https://grapheneos.org/usage
- https://grapheneos.org/faq
- https://www.kuketz-blog.de/grapheneos-der-goldstandard-unter-den-android-roms-custom-roms-teil7/
- Feature-Vergleich von AOSP-Systemen
  https://eylenburg.github.io/android_comparison.htm
- https://www.zdnet.com/article/i-finally-tried-grapheneos-on-my-pixel-and-its-the-secure-android-alternative-ive-been-waiting-for/

Auf Sicherheit getrimmt: GrapheneOS

Matthias Brüstle

Nürnberg 2025-11-23