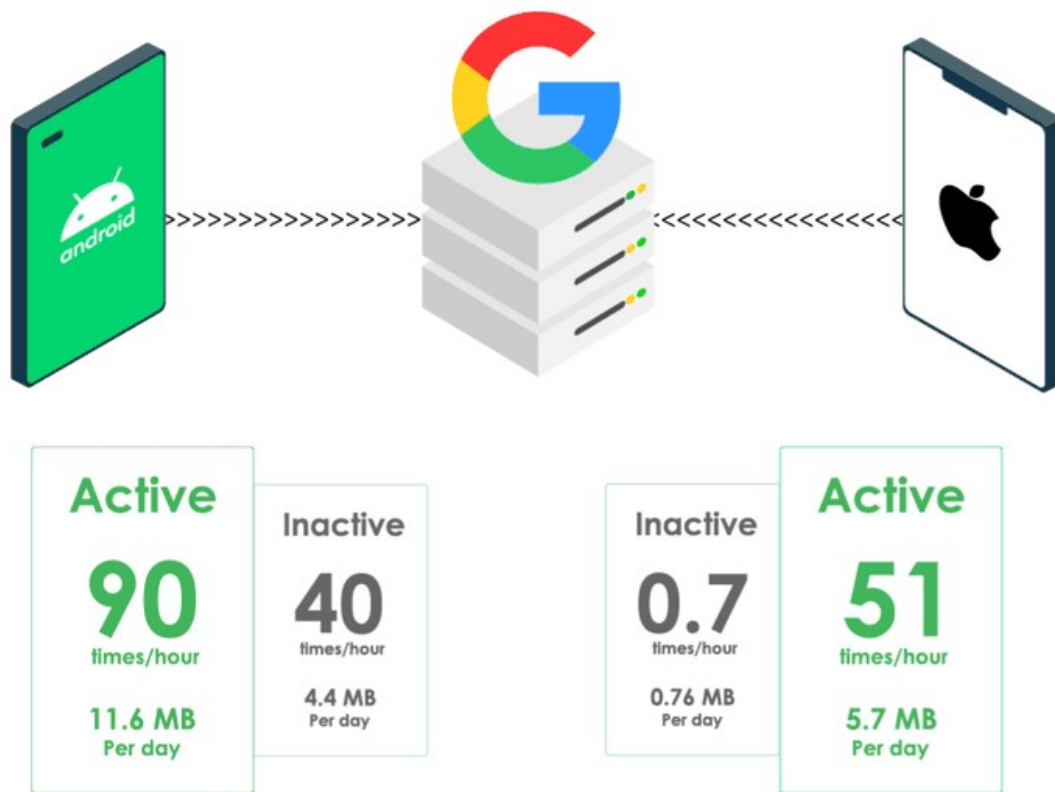


Freiheitshandy – Warum?

Smartphones sind mit Trackern und Software ausgestattet, die den Benutzer überwachen und unnötig viele Informationen an die Hersteller senden. Eine Grafik veranschaulicht das:

Typical day of use



Source: *Digital Content Next* – Prof. Douglas C. Schmidt, Vanderbilt University, August 2018

Das Problem liegt nicht am Smartphone selbst, sondern an dem mitgelieferten Betriebssystem – Android oder iOS. Um die Überwachung zu beenden benötigt es ein Betriebssystem, das keine Daten aussendet. Bei einer Recherche stößt man tatsächlich auf eine Reihe von sog. OpenSource und de-googelten Alternativen. Bei tieferen Recherchen und eigenen Test stellt man schnell fest, dass die meisten Alternativen für Enthusiasten und Entwickler geeignet sind, aber völlig ungeeignet für normale Benutzer. Tatsächlich gibt es nur zwei bzw. drei Alternativen:

- GrapheneOS
- Lineage (/e/OS)

Versucht man ein Smartphone mit einem dieser drei Betriebssysteme bei einem Händler zu kaufen, stellt man fest, dass keine Smartphones mit Lineage verkauft werden. Man benötigt ein kompatibles Smartphone und danach muss man selber das Betriebssystem installieren. Das erfordert vergleichsweise tiefe technische Kenntnisse.

eFoundation

Die eFoundation bietet jedoch /e/OS vorinstalliert auf einem Smartphone an. Die Liste der kompatiblen Typen ist lang – mehr als 100 Geräte <https://doc.e.foundation/devices>. Allerdings bietet die eFoundation nur 5 Geräte out of the Box – also mit dem Betriebssystem zusammen – an: <https://esolutions.shop/>

eFoundation bietet ein rundum Paket an:

- Support und updates garantiert für mehrere Jahre
- volle Kompatibilität mit Android Apps
- Ökosystem basierend auf nextCloud mit Email Account, Kalender, Dateispeicher, Adressverwaltung, Office Paket

Die Benutzung der eCloud ist optional. /e/OS basiert zu 100% auf Lineage. Es gibt zwei Unterschiede:

- microG vorinstalliert (Push notifications)
- Die Bedieneroberfläche (GUI) wurde so umgestaltet, dass sie wie iOS aussieht.

Nitrokey

Die deutsche Firma Nitrokey bietet zwei Smartphones mit vorinstalliertem GrapheneOS an:

https://shop.nitrokey.com/de_DE/shop

Die Benutzeroberfläche ist nahezu identisch zu dem bekannten Android OS von Google. Neben dem Smartphone bietet Nitrokey andere, sehr interessante Produkte aus dem Bereich Security an.

Nachteile:

Der Zugriffsschutz (als bei dem iPhone FaceID) ist deutlich unsicherer. Es wird Passwort und Fingerabdruck angeboten.

Einige Komfortfunktionen fehlen, z.B. Diebstahlschutz. Dies muss mit Hilfe von Apps manuell nachgerüstet werden.

Ich habe das Fairphone 4 mit /e/OS getestet. Der Fingerabdruckscanner ist per se nicht sicher und er ist an einer Stelle am Smartphone eingebaut, die eine sinnvolle Benutzung für mich nicht möglich machten. Daher habe ich fast immer mein Passwort verwendet, um mich anzumelden.

Migrationspfad

Android Smartphone → Nitrokey GrapheneOS (2 Modelle zur Auswahl)

iPhone → eFoundation Smartphone mit /e/OS (5 Modelle zur Auswahl)

Erste Schritte

Nach dem Auspacken und Einschalten des Gerätes läuft eine Initialisierungsroutine ähnlich dem iPhone ab. Man muss Name, eMail Adresse und ein paar andere Eingaben tätigen. Optional kann man hierbei die eCloud konfigurieren (wenn man ein /e/OS Handy hat). Oder später eine andere Lösung konfigurieren.

Nach Beendigung der Initialisierung sollte man sofort den Appstore aufsuchen. Der heißt schlicht „Apps“ (wenn man ein /e/OS Handy hat). Die Bedienung ist sehr ähnlich zum Playstore oder dem AppleStore. Dort installiert man zwei Applikationen: F-Droid und Aurora. Alle weiteren Applikationen sollten aus diesen beiden zusätzlichen Appstores installiert werden. Primär aus F-Droid. Dort befinden sich nur geprüfte de-googelte Applikationen. Wird man dort nicht fündig, kann man mit Aurora auf den kompletten Playstore von Google zugreifen. Aurora bietet einen anonymen Zugriff auf den Playstore, d.h. es müssen keine Benutzerinformationen bei Google hinterlegt werden.