



Meine App-Strategie

Quelle, Profil, Berechtigungen je App · gehört zu Kapitel 7, 8 und 11 · Gerät: _____ · Datum: _____

Die Quelle einer App ist so wichtig wie ihre Berechtigungen. Eine App ist nicht nur Code, sondern auch die Quelle, die bestimmt, wer sie gebaut hat, und die Signatur, die bestimmt, wer Updates ausliefern darf. Unter GrapheneOS gilt: Die Signatur ist die Identität des Entwicklers, jedes Update muss exakt dieselbe tragen. Für Berechtigungen gilt die eine Denkregel: Eine App bekommt nur das, was sie für ihre Kernfunktion zwingend braucht. Alles andere ist Komfort, und dort entstehen die meisten Datenschutzprobleme. Bequemlichkeit ist kein Sicherheitskonzept.

1 · DER ENTSCHEIDUNGSWEG FÜR JEDE NEUE APP (KAPITEL 8)

Nr	Quelle	Kürzel	Was dahinter steckt	Entscheidung
1	GrapheneOS App Store	AS	Vorinstalliert, bewusst kleine Auswahl, eigene Builds. Kein Konto, keine Tracker, keine versteckten Abhängigkeiten.	Nutzen. Das ist der Standard.
2	Accrescent	ACC	Wird aus dem App Store installiert. Entwickler signieren selbst, Accrescent pinnt die Signatur ab der ersten Installation und baut nichts nach. Wenige Apps, das ist das Konzept.	Nutzen.
3	Obtainium (direkte Entwicklerquelle)	OBT	Bezieht die App direkt vom Entwickler, ohne Store dazwischen. Original-Signatur, Updates oft Minuten nach Release. Risiken: falsche Quelle, falsche Prozessorarchitektur, falsche Release-Zuordnung. Die erste Installation ist der Moment, in dem die Signatur geprüft gehört (AppVerifier, Kapitel 11).	Nur, wenn du die Quelle verstehst. Du trägst die Verantwortung selbst.
4	F-Droid	FD	Open Source, aber ein Mittelsmann: F-Droid baut viele Apps selbst und signiert sie mit eigenen Schlüsseln. Updates kommen oft mit Verzögerung.	Abwägen. Für einfache Werkzeuge in Ordnung, für sicherheitskritische Apps nicht die erste Wahl.
5	Aurora Store	.	Lädt aus dem Play Store über geteilte Anonym-Konten, was Googles Bedingungen verletzt und jederzeit ausfallen kann. Zwischenhändler ohne eigene Prüfung, GrapheneOS rät ab.	Alternativen suchen.
R	Zap Store (Radar)	ZAP	Entwickler veröffentlichen direkt, identifiziert über kryptografische Schlüssel statt zentrale Konten. Noch jung, kein Ersatz für die Stufen oben, aber ein gutes Radar für neue, freiheitlich ausgerichtete Apps (Kapitel 13).	Beobachten und ausprobieren.

2 · MEIN BOGEN: EINE ZEILE PRO APP

App	Quelle	Profil	Netz	Stand-ort	Kamera	Mikro	Kon-takte	Spei-cher	Notiz (wofür, was verweigert, was fehlt)
			☐	☐	☐	☐	☐	☐	
			☐	☐	☐	☐	☐	☐	
			☐	☐	☐	☐	☐	☐	
			☐	☐	☐	☐	☐	☐	
			☐	☐	☐	☐	☐	☐	
			☐	☐	☐	☐	☐	☐	
			☐	☐	☐	☐	☐	☐	
			☐	☐	☐	☐	☐	☐	
			☐	☐	☐	☐	☐	☐	
			☐	☐	☐	☐	☐	☐	
			☐	☐	☐	☐	☐	☐	
			☐	☐	☐	☐	☐	☐	
			☐	☐	☐	☐	☐	☐	
			☐	☐	☐	☐	☐	☐	

Quelle: AS = GrapheneOS App Store · ACC = Accrescent · OBT = Obtainium, direkt vom Entwickler · FD = F-Droid · ZAP = Zap Store · PLAY = Sandboxed Google Play (nur, wenn die App ohne nicht läuft)

Profil: H = Hauptprofil · V = Vertrauliches Profil · N: ____ = eigener Nutzer, mit Kürzel (Kapitel 15)

Kästchen: leer = verweigert · X = erlaubt · U = nur während der Nutzung · beim Standort zusätzlich ~ = nur ungefähr. Kamera und Mikrofon nie dauerhaft, Speicher nur den zugewiesenen Ordner (Storage Scopes), Kontakte nur ein leeres oder minimales Adressbuch (Contact Scopes).

⚠ **Netz ist unter GrapheneOS eine eigene Berechtigung.** Nur erlauben, wenn die Kernfunktion online liegt. Eine Taschenlampe oder ein Taschenrechner mit Internetwunsch ist eine rote Flagge (Kapitel 7). ⚠ **Signaturwechsel bei einem Update ist ein Warnsignal.** Entweder hat der Entwickler den Schlüssel verloren oder jemand anderes liefert plötzlich Code aus. Beides ist ein Problem. Android verweigert das Update dann. Nicht deinstallieren und neu installieren, sondern Quelle prüfen (Kapitel 8). ⚠ **Google-abhängige Apps gebündelt in genau einem Bereich.** Sandboxed Google Play einmal installieren, entweder im Vertraulichen Profil oder in einem eigenen Nutzer, und alle Apps, die es brauchen, dorthin. So wenige Google-Instanzen wie möglich (Kapitel 15).

Bewusst kein Feld für Konten, Nutzernamen oder Passwörter. Dieses Blatt darf gefunden werden, ohne dass es etwas verrät.