

Geheime Schutzinselprofile

zweite



A futuristic smartphone displaying a hidden „Second Space“ profile designed to conceal sensitive data, sci-fi cyber security aesthetic, dual digital identities inside one device, encrypted private zone glowing beneath the normal interface, holographic folders, hidden emails and secret files protected behind biometric locks, layered user profiles visualized as parallel digital realities, dark neon environment, blue and cyan light, cinematic atmosphere, ultra-detailed, cyberpunk style, advanced mobile privacy technology, glowing encryption symbols, realistic high-tech smartphone UI, dramatic volumetric lighting, octane render, 8k –ar 16:9 –stylize 700

Wir müssen es mit der Datencontainerwissenschaft noch weiter treiben, zumal in den Kommentaren [Defätismus](#) verbreitet wurde, dem ich entgegenwirken will.

Die Idee, auf mich und meine [kleine Hirse gemünzt](#) (ich habe jetzt zwei Xiaomi-Handys): Ist es möglich, das E-Mail-Programm – hier [FairEmail](#) – in einem geschützten Container zu betreiben?

Die KI sagt: Ja und nein. Es sei prinzipiell möglich, „aber mit wichtigen Einschränkungen unter Xiaomi Android bzw. [HyperOS/MIUI](#).“

Programme wie [EDS](#) können verschlüsselte Container (ähnlich VeraCrypt) bereitstellen. Darin lassen sich Dateien speichern. Schwieriger wird es aber bei kompletten installierten Apps wie

FairEmail.

Der entscheidende Punkt: Android installiert Apps normalerweise immer im regulären App-Bereich des Systems. Ein Container wie EDS kann zwar APK-Dateien oder Daten speichern, aber nicht ohne weiteres eine App „unsichtbar“ im Container betreiben, sodass sie erst nach dem Mounten erscheint.

Vorschlag: eine „Work Profile“-Container benutzen.

Mit Apps wie [Shelter](#), [Insular](#) oder [Island](#) kann man FairEmail in ein getrenntes Arbeitsprofil installieren. Dieses Profil kann gesperrt werden. Dann verschwindet die App aus dem normalen Bereich, Benachrichtigungen stoppen, und erst nach Entsperren des Profils wird FairEmail sichtbar.

Alle drei Apps – Shelter, Insular und Island – basieren auf derselben Android-Technik: dem sogenannten „Work Profile“ bzw. Arbeitsprofil. Sie erzeugen also keinen echten VeraCrypt-artigen Container, sondern nutzen die von Android eingebaute Trennung verschiedener Profile.

„Das ist auf Xiaomi-Geräten meist die praktikabelste Lösung ohne Root-Zugriff.“

Funktion	Shelter	Insular	Island
Open Source	Ja	Ja	Teilweise / nicht vollständig FLOSS
Basis	Eigenständiges Projekt	Fork von Island	Originalprojekt
Datenschutz-Fokus	Sehr hoch	Hoch	Mittel
Werbung / Tracking	Keine bekannt	Keine bekannt	Teilweise Google-näher
Bedienung	Einfach, technisch	Modern und komfortabel	Sehr komfortabel

Funktion	Shelter	Insular	Island
Apps einfrieren („Freeze“)	Ja	Ja	Ja
Arbeitsprofil pausieren	Ja	Ja	Ja
Kontakte zwischen Profilen blockieren	Gut	Sehr gut	Eher schwach
F-Droid verfügbar	Ja	Ja	Nein
Xiaomi-Kompatibilität	Meist gut	Gut	Schwankt je nach HyperOS-Version
Ressourcenverbrauch	Gering	Mittel	Mittel
Typische Zielgruppe	Privacy- und Security-Nutzer	Privacy mit mehr Komfort	Mainstream- und Komfort-Nutzer
Besonderheit	Sehr transparent und minimalistisch	Guter Mittelweg zwischen Privacy und Bedienung	Viele Komfortfunktionen und App-Klonen
Empfehlung für FairEmail auf Xiaomi	Sehr empfehlenswert	Gut geeignet	Eher Komfortlösung

[Eine Stunde später.] Nein, ist es nicht.

Auf Xiaomi-Smartphones lässt sich Shelter zwar per [F-Droid](#) installieren, aber die vollständige Installation wird geblockt. Shelter ist auch im Play Store nicht mehr erhältlich. Shelter und Insula [wurden entfernt](#), „unter anderem wegen Android-/Google-Play-Richtlinien rund um Work Profiles und App-Installation.“

Ich kann natürlich nichts darüber sagen, wie Apps, die per F-

Droid installiert wurden, auf Samsung- und anderen Smartphones funktionieren. Bei Xiaomi geht es definitiv nicht.

Zwischen Haupt- und
Zweitprofil wechseln



Also Plan B. Und der wird jetzt richtig kompliziert und nerdig, aber es funktioniert.

Wer sich aber der Hilfe der KI bedienen will, muss starke Nerven haben, weil auf Anhieb alle Antworten falsch sind und dann bedauernd kommt: Ja, tut mir leid, früher war das so, heute ist das nicht mehr der Fall und ähnlicher nervtötender Quatsch.

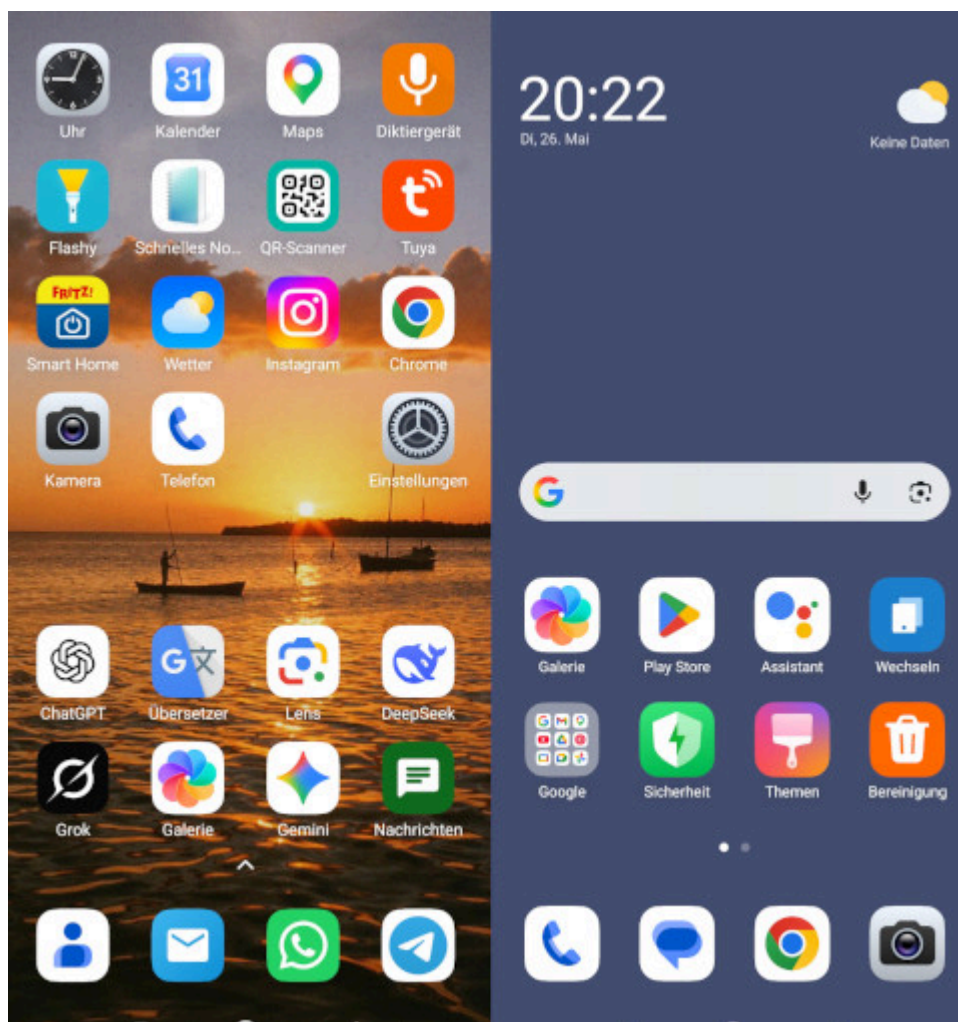
Man muss ein so genanntes Zweitprofil einrichten. (Die Option findet man in den Einstellungen.)

HyperOS hat die Oberfläche von „Second Space“ stark verändert:

- manche Regionen blenden das Icon aus,
- manche zeigen es nur im Zweitprofil,
- manche nur über den Sperrbildschirm.

Das ist an sich nicht kompliziert (wenn man das Feature gefunden hat). Die Panik kommt, wenn es funktioniert und man plötzlich vor einem ganz „fremden“ Handy-Monitor mit nur wenigen Apps sitzt. Wie gelangt man wieder zurück ins Hauptprofil? Es gibt im Zweitprofil einen „Schalter“ (wie eine App) „wechseln“. Aber mitnichten im Hauptprofil.

Man muss tricksen: Den Bildschirm sperren und dann mit dem Passwort oder dem Fingerabdruck des Zweitprofils einloggen. Niemand weist einen darauf hin, dass man beim Anlegen des zweiten Profils auch andere Passwörter benutzen sollte – sonst funktioniert das nicht und man tritt|tippt auf der Stelle.



Ich finde die Idee gut. Es ist fast so wie bei einem *hidden container*: Wenn ein Schnüffler gar nicht weiß, dass es ein zweites Profil gibt, müsste man schon gezielt und lange – mit forensischen Methoden – danach suchen. (Den Button „Wechseln“ habe ich ganz nach hinten verbannt.)

Wie die Übersicht unten zeigt, bieten einige Hersteller diese Option an.

Kompliziert ist bei Xiaomi, Daten von einem Profil zum anderen zu schicken. Ich habe mir beim ersten Mal mit Webmail beholfen. Zukünftig werde ich – wie bisher – einfach FTP

benutzen.

Hersteller	Funktion	Art der Trennung	Besonderheiten
Xiaomi	Zweitprofil / Second Space	Sehr stark	Fast wie ein zweites Smartphone mit getrennten Apps, Daten und Konten
Samsung	Secure Folder	Stark	Knox-basierte Hardwareverschlüsselung, separater geschützter Bereich
OnePlus	System Cloner / Private Safe	Mittel bis stark	Separates Benutzerprofil mit eigenen Apps und Daten
OPPO	Privacy Space / System Cloner	Stark	Ähnlich Xiaomis Zweitprofil, inklusive separater Apps und Konten
Vivo	Privacy Space	Mittel	Fokus auf versteckte Apps und private Datenbereiche
Huawei	PrivateSpace	Sehr stark	Komplett getrenntes Profil mit eigenem Passwort und Fingerabdruck
Honor	Parallel Space / Private Space	Mittel	Je nach MagicOS-Version unterschiedlich umfangreich
Google Pixel / Android 15+	Private Space	Mittel	Versteckter App-Bereich mit separater Sperre und eigenem Play Store

Hersteller	Funktion	Art der Trennung	Besonderheiten
Standard-Android vieler Hersteller	Gastmodus / Mehrbenutzer	Sehr stark	Echte Android- Benutzerkonten mit vollständiger Trennung
Beste Sicherheitslösung	Samsung Knox Secure Folder	Sehr stark	Besonders starke Hardware- und Software- Isolation
Beste Alltagstauglichkeit	Xiaomi Zweitprofil	Sehr stark	Sehr komfortabler Wechsel zwischen getrennten Bereichen