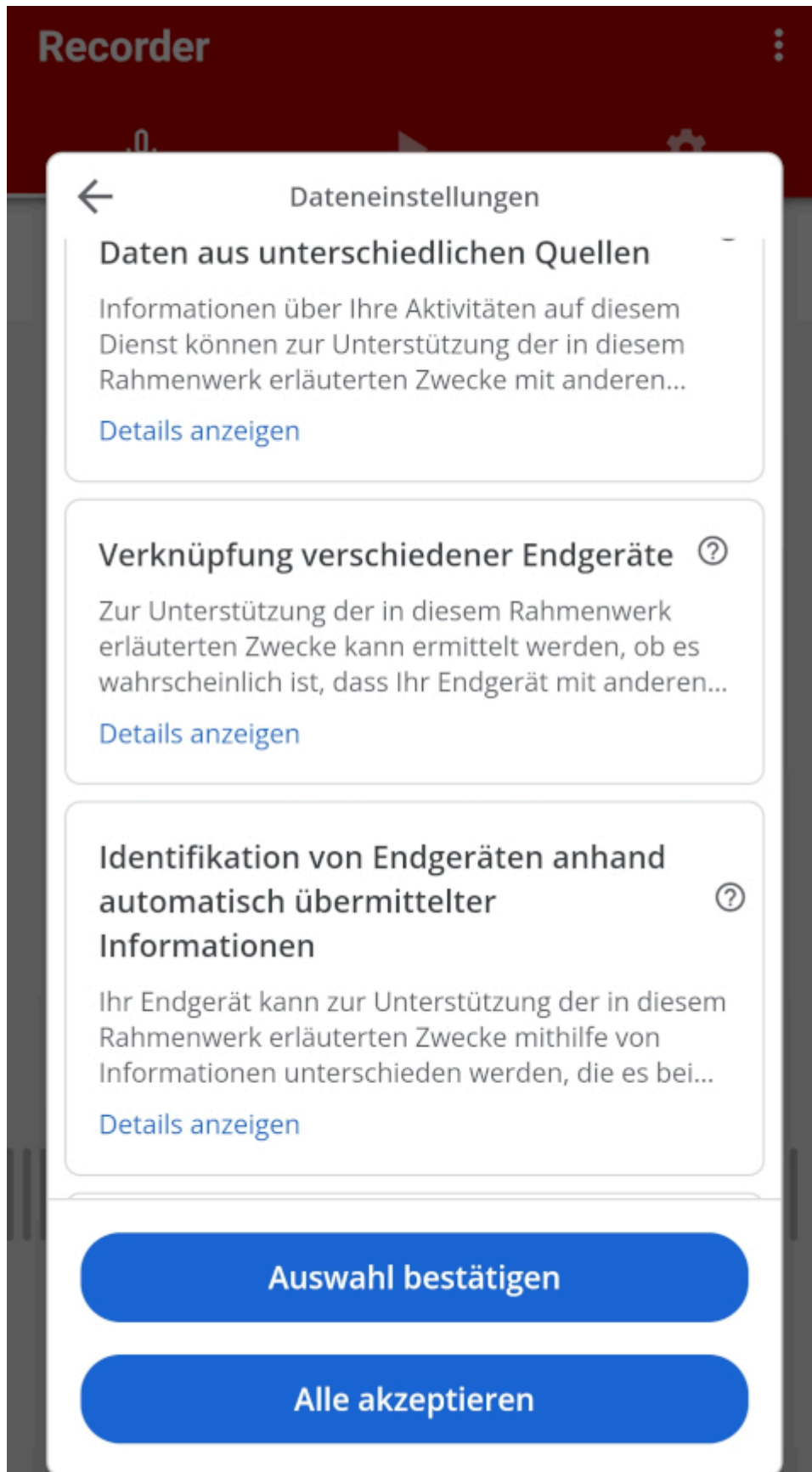


□□ oder kleine Hirse [Update], revisited




Ich bin erst jetzt dazu gekommen, meine [kleine Hirse](#) genauer anzuschauen und alles zu installieren oder auch rauszuwerfen, was für mich nötig ist. Wenn man die Sache ernst nimmt, dauert das Stunden. Sogar [einfache Aufgaben](#) kriegt man nicht spontan hin, sondern nur mit Herumfummeln. Ich kann mir nicht vorstellen, dass „normale“ Handy-Nutzer dazu Zeit und Lust haben. Zum Glück bin ich nicht normal. Ich lesen sogar überflüssige und nichtssagende [Bedienungsanleitungen](#).

Die Conclusio ist natürlich, dass Smartphones nicht wirklich sicher sein können, außer man benutzt teure [Spezialmodelle](#) [Jan, ihr könntet die Werbung mal ein bisschen variieren!], sondern Datenschleudern bleiben, von denen man nicht wirklich weiß, was sie tun.

Die Hakelei [fing bei Keepass an](#): „Ungültiger zusammengesetzter Schlüssel“. Das Übliche halt – Beamen von [komischen Dateien](#) zwischen verschiedenen Betriebssystemen ist nichts für Anfänger. Ich werde zuhause, falls ich in den nächsten Tagen eine halbe Stunde Zeit finde, was unwahrscheinlich ist, den Hauptrechner direkt an das Smartphone anschließen. Eigentlich müsste ich auch noch einen [EDS-Container anlegen](#). Das spare ich mir für lange Winterabende auf.

Das [Xiaomi 13T Pro](#) hat alle Apps, die ich schon besaß, brav kopiert. Nur [F-Droid](#) und die damit verbundenen Open-Source-Apps musste ich händisch nachinstallieren. Auch die hier schon empfohlenen [SHOKZ OpenFit True Wireless Earbuds](#) wurden sofort erkannt. Signal hingegen wollte zum Beispiel die Daten vom alten Gerät nicht übertragen.



Alle Optionen haben häufig verwendete Standardwerte, die für die Verwendung der App nicht geändert werden müssen 

Allgemein



Die Standardmethode zum Verschlüsseln (PGP oder S/MIME) wird nach dem Senden einer signierten oder verschlüsselten Nachricht für jede Identität einzeln gespeichert. Die Verschlüsselungsmethode kann vor dem Senden in den Sendeoptionen ausgewählt werden (»Senden« gedrückt halten).

- Standardmäßig signieren
- Standardmäßig verschlüsseln
- Automatisch verschlüsseln, wenn alle Empfängerschlüssel verfügbar sind
- Signierte Nachrichten automatisch überprüfen
- Nachrichten automatisch entschlüsseln
- Unterhaltung beim Schließen erneut verschlüsseln

Ausgewählte Schlüssel zurücksetzen 

Kann im Falle von neuen Zertifikaten usw. verwendet werden.

ChatGPT schreibt einen halben Roman als Antwort auf die Frage: „Wenn ich auf einem Handy der Marke Xiaomi 13t das E-Mail-

Programm FairEmail benutze und die App OpenKeychain, wie gehe ich am besten vor, wenn ich ein schon vorhandenes PGP-Schlüsselpaar importieren will und es in einem Dateiordner von Android speichern will, auf den keine anderen Apps Zugriff haben soll?“

Aber dort ist nichts, was ich nicht schon wüsste, zum Beispiel:

Speicherort für das Schlüsselpaar festlegen:

Um die Datei in einem sicheren Ordner zu speichern, der für andere Apps nicht zugänglich ist, können Sie den internen Speicher Ihres Telefons verwenden.

Eine Möglichkeit ist, die Datei in den internen Speicher zu verschieben und sicherzustellen, dass sie nicht im öffentlichen Download-Ordner verbleibt.

Sie können auch einen spezifischen Ordner erstellen und diesen mit geeigneten Zugriffsrechten versehen.

Zugriffsrechte Einschränken:

Um sicherzustellen, dass keine anderen Apps auf Ihren Schlüssel zugreifen können, überprüfen Sie die App-Berechtigungen auf Ihrem Xiaomi-Gerät.

Gehen Sie zu „Einstellungen“ > „Apps“ > „App-Berechtigungen“ und stellen Sie sicher, dass nur OpenKeychain und FairEmail die notwendigen Berechtigungen haben.

Erwägen Sie, die Datei mit Ihrem Schlüsselpaar in einem spezifischen Ordner zu speichern, der versteckt ist oder für andere Apps nicht zugänglich gemacht wird.

Sobald die [Hülle](#) von der Großbourgeoisie wird geschickt worden sein (das seltene [Futur II!](#)), werde ich dann auch die Sim-Karte von alt nach neu ~~teleportieren~~ hinüberdröseln.

Datensicherheit



Was die Sicherheit angeht, solltest du als Erstes verstehen, wie Entwickler deine Daten erheben und weitergeben. Die Datenschutz- und Sicherheitspraktiken können je nach deiner Verwendung, deiner Region und deinem Alter variieren. Diese Informationen wurden vom Entwickler zur Verfügung gestellt und können jederzeit von ihm geändert werden.



Diese App kann die folgenden Datentypen an Dritte weitergeben
App-Informationen und -Leistung und Geräte- oder andere IDs



Diese App kann die folgenden Datentypen erheben
App-Informationen und -Leistung und Geräte- oder andere IDs



Daten werden bei der Übertragung verschlüsselt



Die App bietet keine Möglichkeit, das Löschen von Daten zu beantragen