



Signatur-Anker – meine Wallet-Software

Schlüssel-Fingerprints der eigenen Programme, einmal geprüft, dauerhaft notiert · gehört zu Kapitel 3 und 6

Warum Fingerprints statt Prüfsummen: Die SHA-256 einer Datei ist versionsgebunden und ändert sich mit jedem Release – sie wird bei jedem Update frisch geholt und gegen die Signatur geprüft. Der Fingerprint des Signaturschlüssels dagegen ist der dauerhafte Anker: Er wechselt praktisch nie, und ein Wechsel ist ein Ereignis, das der Hersteller mehrfach öffentlich ankündigt. Dieses Blatt ist deine eigene Aufzeichnung – beim nächsten Update vergleichst du gegen dein Papier statt gegen das Internet. **Merksatz:** Hash weicht ab und Signatur hält → Problem der Webseite. Hash passt und Signatur bricht → Alarm.

So füllst du das Blatt aus: Fingerprint des Herstellerschlüssels über **mehrere unabhängige Kanäle** prüfen (Hersteller-Webseite, offizielle Doku, Entwickler-Profile), erst wenn alle übereinstimmen hier eintragen, mit Datum und den geprüften Kanälen. Ein Kanal allein genügt nicht – und die Kurz-ID (die letzten 16 Stellen) ist kein zweiter Beleg, sondern derselbe Wert in kurz.

MEINE SIGNATUR-ANKER

Programm / Hersteller	Fingerprint (40 Stellen, in Vierergruppen)	Ablaufdatum	Geprüft bei (Kanäle) + Datum

⚠ „Korrekte Signatur“ allein genügt nicht. Die Meldung heißt nur: irgendein Schlüssel aus deinem Schlüsselbund hat unterschrieben. Entscheidend ist, dass der Fingerprint des signierenden Schlüssels mit deinem Eintrag auf diesem Blatt übereinstimmt. ⚠ **Trägt ein Schlüssel ein Ablaufdatum**, gehört der Termin in den Kalender – nach dem Ablauf meldet die Prüfung eine abgelaufene Signatur, und das ist dann weder Angriff noch Fehler, sondern der erwartete Schlüsselwechsel.

UPDATE-LOG

Datum	Programm	Version	Signatur geprüft, Fingerprint stimmt	Bemerkung

Dieses Blatt enthält nur öffentliche Werte (Fingerprints signierender Schlüssel) – trotzdem gilt: keine Seeds, keine Passphrasen, keine xpubs darauf notieren

alien-investor.org · v0.1 Prototyp · Stand 2026-08-31 · CC BY-SA 4.0