Signature anchors – my wallet software

The signing-key fingerprints of your own programs, checked once, recorded for good · belongs to chapters 3 and 6

Why fingerprints instead of checksums: A file's SHA-256 is bound to one version and changes with every release – it is fetched fresh at every update and checked against the signature. The fingerprint of the signing key, by contrast, is the durable anchor: it practically never changes, and a change is an event the vendor announces publicly several times over. This sheet is your own record – at the next update you compare against your paper instead of against the internet. **Rule of thumb:** hash differs and the signature holds → a website problem. Hash matches and the signature breaks → alarm.

How to fill in this sheet: Check the vendor key's fingerprint across **several independent channels** (vendor website, official documentation, developer profiles); only when all of them agree do you enter it here, with the date and the channels you checked. One channel alone is not enough – and the short key ID (the last 16 characters) is not a second proof, it is the same value in short form.

MY SIGNATURE ANCHORS

Program / vendor	Fingerprint (40 characters, in groups of four)	Expiry date	Checked at (channels) + date

⚠ **"Good signature" alone is not enough.** That message only means: some key from your keyring signed. What matters is that the fingerprint of the signing key matches your entry on this sheet. ⚠ **If a key carries an expiry date,** the date belongs in your calendar – after expiry the check reports an expired signature, and that is then neither an attack nor a bug but the expected key rollover.

UPDATE LOG

Date	Program	Version	Signature checked, fingerprint matches	Notes