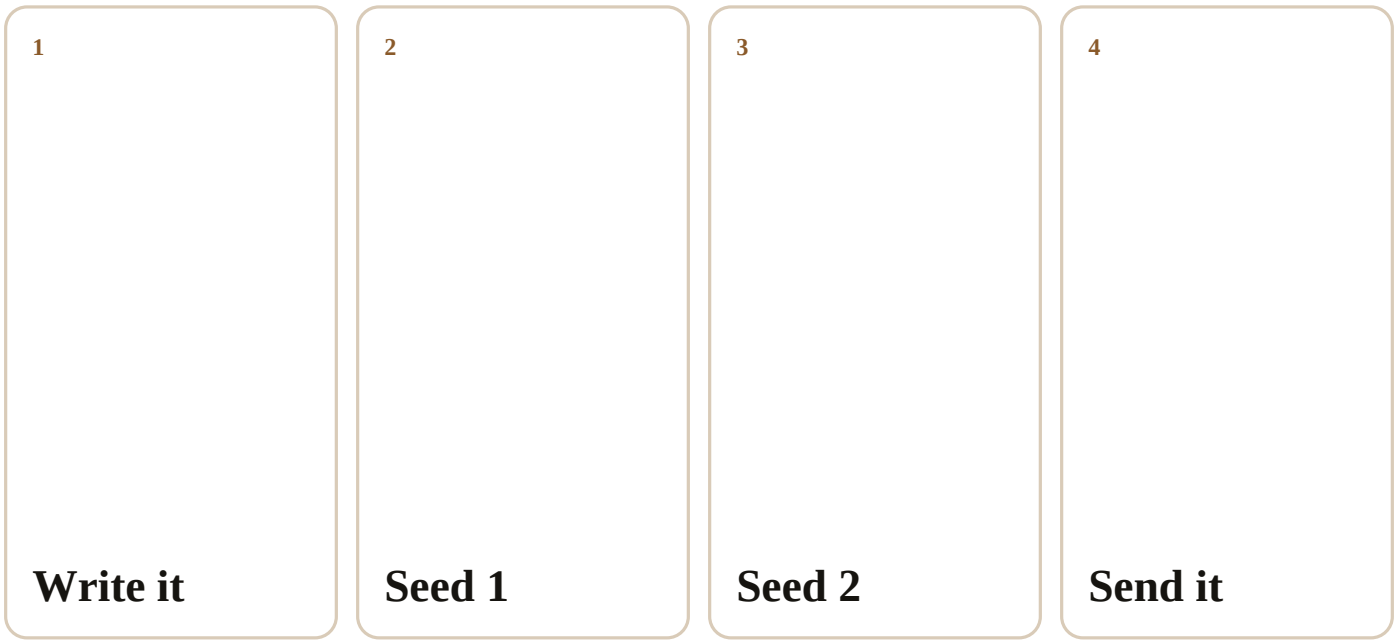
The second signature is a new boot. Seed 1 is not still in memory. Seed 3 is not loaded unless one of the other keys is gone.



Then the payment can move

Tails is booted again, with networking set to Disabled. Seed 2 is the only seed loaded. The partially signed file is opened, the second signature is added, and the finished file is copied out.

The everyday computer opens that file and broadcasts it only after both signatures are present. The destination and the amount are checked against the note that was written down before the first signature.

Seed 3 stays boxed. It is used only if seed 1 or seed 2 is gone. Two seeds are never loaded in one session.