SOVERIS

SOVEREIGN CUSTODY

WHITE PAPER · 2026

Sovereignty, by design.

How a foundation that cannot betray you — and guard rails you set yourself — let you hold significant digital assets without the conflicts of an exchange or the fragility of self-custody. By design, not by contract.

Pure sovereignty. Zero conflicts of interest. Full control.

Version 1.0 — June 2026
soveris.de
Informational. Not legal or financial advice.

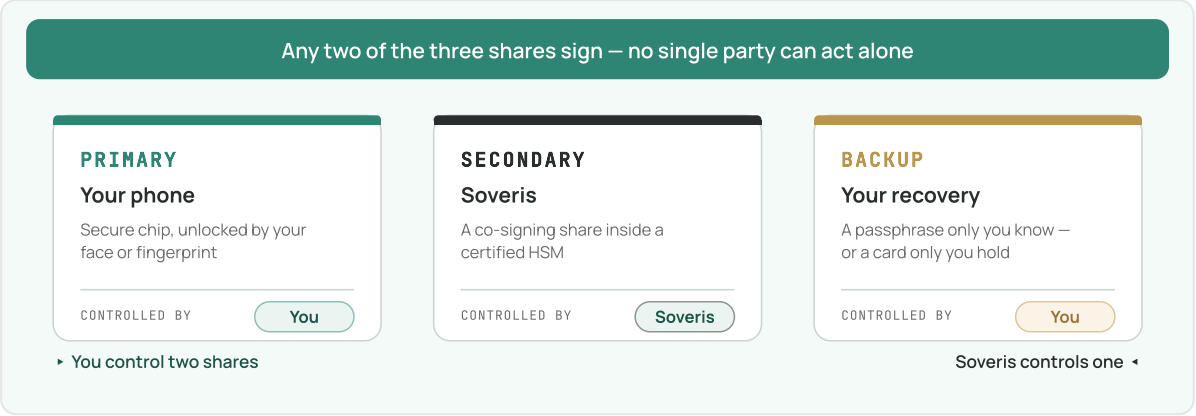
Neither taken from you, nor lost by you.

There are only two ways to lose digital wealth: someone takes it from you, or you lose it yourself. Almost every product ever built protects you from one of these by exposing you to the other.

At one end sit the exchanges and custodians. They hold your assets — and often trade, lend, or pledge them to fund their own business. You become an unsecured creditor, your withdrawals can be frozen, and a single insolvency or breach can take everything. At the other end sits pure self-custody. No one can take your assets, but a lost seed phrase, a sudden death with no succession, or a moment of physical coercion can erase them just as completely. The sophisticated holder has been asked to choose which way to lose.

Soveris is engineered to be the one position exposed to neither end. Not through a better promise, a larger balance sheet, or a licence — through a single structural decision, and a layer of protection you build on top of it.

Your wallet is protected by three independent key shares. Any two of them, working together, can authorise a transaction. No single party ever holds enough to act alone. You hold two of the three: one inside your phone's secure hardware, protected by your fingerprint or face; one as your private backup, which you alone control. Soveris holds the third, in a hardware security module. The complete signing key is never assembled — on any device, at any moment, including while you sign.



From that one fact, everything follows:

- **Soveris cannot act alone.** One share of three can do nothing. This is not a policy we promise to keep; it is a structural property of the threshold design. We cannot betray you, because we cannot act without you.
- **You can always leave.** Your two shares move your assets to any wallet you choose, with no cooperation from Soveris — even if Soveris ceased to exist tomorrow.
- **Losing your phone is not losing your wealth.** A new device is restored in minutes, not days, with your backup untouched. The hard cases — death, incapacity, a lost passphrase — each have a defined, lawyer-friendly path.
- **Your estate is provided for.** Under German succession law, where Soveris is established, your heirs become the account holder through a defined succession process. No seed phrase passed across a kitchen table; no crypto literacy required of the people you leave behind.
- **No conflict of interest is possible.** No trading desk, no lending book, no staking of your coins — and by the architecture itself, Soveris cannot move your assets to earn from them. Alignment is structural, not promised.

That foundation is only half of the design. On top of the two-of-three foundation sits a layer of *guard rails* you configure yourself: a ceiling on what moves in a single transaction and across a day, a delay before a newly added recipient can be paid, a hold on withdrawals, a time-lock on releasing your backup that defeats coercion, and a check-in mechanism that carries your wealth safely through incapacity and inheritance. The foundation makes Soveris incapable of betraying you; the guard rails make the everyday use of your own wealth both effortless and safe — a single biometric gesture for the ordinary day, and a wall of your own design between an attacker and your estate on the worst one.

Where Soveris stands in law. Because you alone control your assets, and you alone initiate and broadcast every transaction, Soveris is built to operate as a non-custodial software and MPC-infrastructure provider rather than a crypto-asset custodian — a position we set out plainly later in this paper and are confirming with qualified counsel. Soveris provides the cryptographic tools; the sovereignty is yours.

No system removes every risk, and this paper will not pretend otherwise. The pages that follow set out the architecture, the guard rails in detail, the recovery and succession paths, the cryptography, the regulatory standing, and — plainly — the limits of what we can protect you from.

1 The Custody Dilemma

Ask anyone who has held digital assets for long enough what keeps them awake, and you will hear one of two fears. Either *someone will take it* — the exchange collapses, the custodian lends out the coins, the withdrawal button stops working. Or *I will lose it myself* — the recovery phrase is misplaced, the holder dies and the wealth dies with them, or a thief at the door forces a transfer in seconds.

These are not two versions of the same risk. They pull in opposite directions, and that is the heart of the problem.

When you hand your assets to a custodian, you are protected from yourself. You cannot misplace a key you never held; if you forget your password, the custodian resets it. But you have taken on a counterparty. The custodian's business may depend on using your assets — trading them, lending them, pledging them. If the custodian fails, you stand in line with every other creditor. The custodial collapses of recent years were not exotic failures; they were the predictable consequence of letting one party hold both the assets and the incentive to use them.

When you take full self-custody, you remove the counterparty entirely. No one can freeze your assets, lend them, or seize them through a court order served on someone else. But every failure is now yours alone. A lost backup is permanent. A death with no succession plan erases the estate. A coercion attack succeeds in the time it takes to read out a phrase, because nothing stands between the threat and the transfer.

Soveris is engineered to sit at the one point exposed to neither end.

Loss is a spectrum. Every other product optimises one end and fails the other. The 2-of-3 split separates "who can move it" from "who can recover it", so Soveris is exposed to neither failure mode.

Every product is a point on this line. Move toward safety from theft and you move toward exposure to self-loss; move toward protection from self-loss and you move back toward a counterparty. Collaborative-custody services have done genuine work to occupy the middle. But the middle they reach is still a compromise: largely Bitcoin-only, often demanding real technical fluency from the holder and their heirs, and rarely designed around European law or European estates.

Soveris was built to occupy a single point on this line that is exposed to neither end. The mechanism that makes that possible is the subject of the next section.

---

2 The Foundation: How Soveris Works

The whole design rests on one idea, so it is worth stating slowly.

Your wallet is governed by **three independent key shares**. Cryptographers call this threshold cryptography, or multi-party computation — MPC for short. A transaction is authorised when **any two of the three shares** take part in signing it. No single share is ever enough. And — this is the part that matters

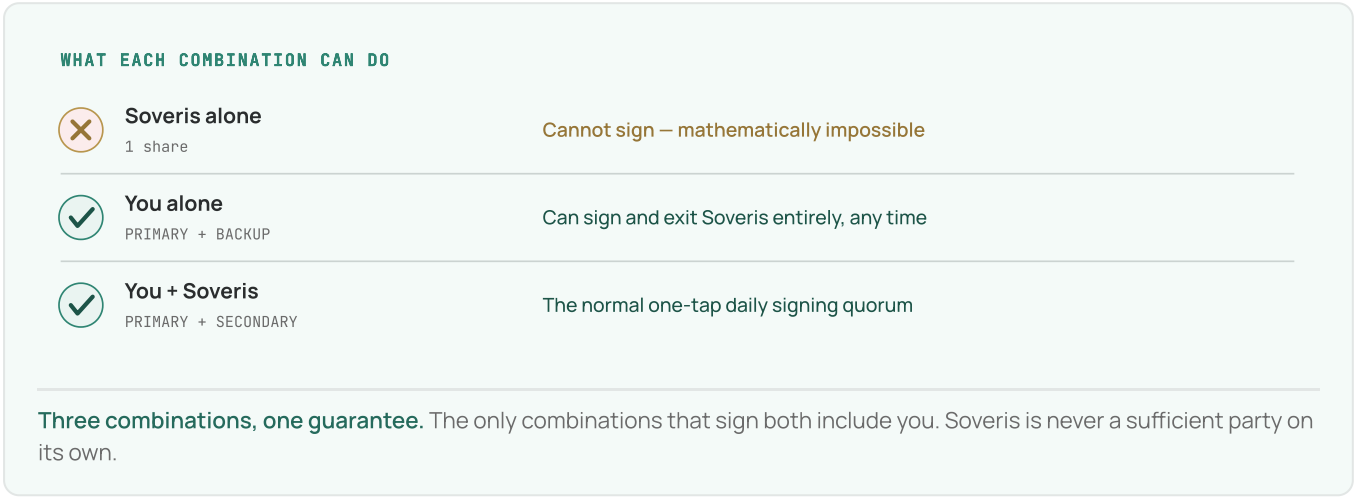
most — the complete signing key is never assembled anywhere: not on your phone, not on our systems, not for an instant during signing. Each share is, on its own, a useless fragment.

The three shares have distinct roles and distinct guardians.

Share	Where it lives	What protects it	Who controls it
PRIMARY	Inside your phone's hardware secure element — the Secure Enclave on iPhone, StrongBox on Android	Hardware isolation plus your fingerprint or face; it never leaves the secure element in readable form	You
SECONDARY	A Soveris-operated hardware security module (HSM)	A FIPS-certified HSM, with each customer's key material kept fully separate	Soveris
BACKUP	Your choice: a *Knowledge* form (an encrypted record openable only with your Recovery Passphrase) or an *Ownership* form (a physical secure-element card you keep)	Knowledge: a memory-hard passphrase encryption. Ownership: the card's secure element and PIN	You

You always hold two of the three: PRIMARY on your phone, and BACKUP wherever you keep it. That is the basis for the word *sovereign*. Three statements follow directly, and the entire foundation is contained in them:

- **Soveris alone, with one share, cannot sign.** It is not that we choose not to — by the design of the threshold scheme, a single share of three cannot produce a signature. We cannot act without you.
- **You alone, with PRIMARY and BACKUP, can sign — and can leave at any time**, with no participation from Soveris whatsoever.
- **You and Soveris together, with PRIMARY and SECONDARY, form the everyday quorum** that signs your daily transactions.



Throughout, one principle holds without exception: **you initiate every transaction, and you alone broadcast it to the network.** Soveris contributes its co-signing share only when you authorise an action you have started. Soveris never initiates a transaction in your name, and Soveris never broadcasts. Without your action, nothing happens.

The cryptography, stated plainly

Soveris uses modern, peer-reviewed threshold-signature schemes, deliberately chosen to avoid older schemes associated with known vulnerability classes. The signatures the system produces are ordinary signatures on the blockchain — indistinguishable from those of a single-key wallet, and supported across many chains rather than a single one.

The on-device PRIMARY share is held in the phone's hardware secure element, gated by biometrics and managed by the operating system; it is never exported in readable form. It is worth being precise about one point that technical readers will check: **your fingerprint or face is never used to derive any encryption key.** Biometrics are an operating-system convenience that unlocks the on-device share for daily signing. The portable cryptographic anchor is your account password, never your biometric, which is bound to one device and cannot travel.

The Soveris HSM is FIPS-certified, on a path toward a dedicated FIPS 140-3 Level 3 module. Each customer's key material is fully separated from every other customer's, and is wrapped with AES-256-GCM. The HSM only ever sees its own SECONDARY share and the shared public key; it never sees PRIMARY or BACKUP.

The Knowledge BACKUP is encrypted with XChaCha20-Poly1305 authenticated encryption, under a key derived from your Recovery Passphrase using Argon2id — a memory-hard key-derivation function chosen specifically to make brute-force attack expensive, even against specialised hardware. Soveris stores only the resulting ciphertext and a non-secret random value; **Soveris cannot derive the key and cannot decrypt the record.** Each encrypted record is cryptographically bound to its version and to your wallet's public-key fingerprint, which prevents replay, rollback, or substitution attacks.

Roughly every ninety days — and immediately on any security event — the shares are mathematically refreshed, with your phone taking part in the routine cycle. The public key and your wallet address are preserved unchanged, but the previous shares become cryptographically invalid, even if an attacker had quietly retained one. This caps the window during which any single compromised share could matter.

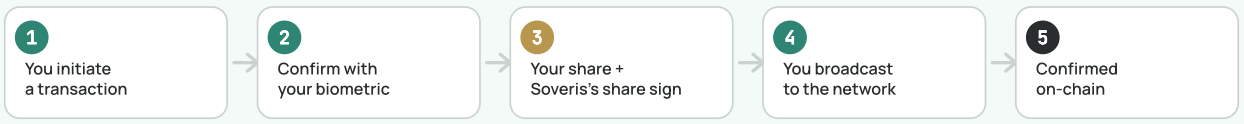
Finally, you are not asked to take our word for what we hold on your behalf. Each customer has dedicated on-chain addresses, verifiable on any block explorer, by anyone, at any time. We call this *proof of holdings*, and it is stronger than the periodic *proof of reserves* an exchange might publish: yours is continuous, permissionless, and specific to you, not a pooled snapshot you must trust.

No vendor lock-in sits anywhere in this picture. Every external component is substitutable; the cryptographic guarantee that you can always exit does not depend on any single supplier.

3 A Day with Soveris

Sovereignty should not feel like a discipline. In daily use, it feels like unlocking your phone.

You open the app and prepare a transaction — an amount, a recipient. You confirm with your fingerprint or face. Behind that single gesture, your phone's PRIMARY share and the Soveris HSM's SECONDARY share run a brief signing exchange, and the completed signature is assembled on your device. Your app then broadcasts the signed transaction to the network — through a public relay, your own node, or any channel you prefer. There is no seed phrase to type, no password to enter at signing time, no separate hardware device to find. The gesture is the same one you already use for a banking app.



A normal signature. One biometric gesture — no seed phrase, no hardware ritual. Soveris contributes its co-signing share only after you authorise, and never broadcasts: you hold and publish the final signed transaction.

To be exact about who does what: you initiate the transaction, you authorise it with your biometric, and your device holds and broadcasts the final signed transaction. Soveris contributes one co-signing share when you ask, and contributes nothing otherwise.

When you change phones

A new phone is the most common real-world event, and it is deliberately undramatic. You install the app and log in with your account password, then re-register your biometrics. The encrypted backup of your PRIMARY share is fetched and decrypted locally, on your device, using your account password — which never reaches Soveris. The share is then re-sealed into your new phone's secure element. Your BACKUP share is not touched. The target is under a minute.

The two things to remember

For your entire life with Soveris, you hold exactly two secrets. Everything else — biometrics, app sessions, device pairings — is convenience that any new device can rebuild.

- An **account password**, like any other login. It can live in a password manager, and it is the secret that anchors a move to a new device.
- A **Recovery Passphrase**, written down once at signup and kept where you keep important documents — with your will, in a safe, or with your lawyer. You will rarely, if ever, type it; it exists for the exceptional cases.

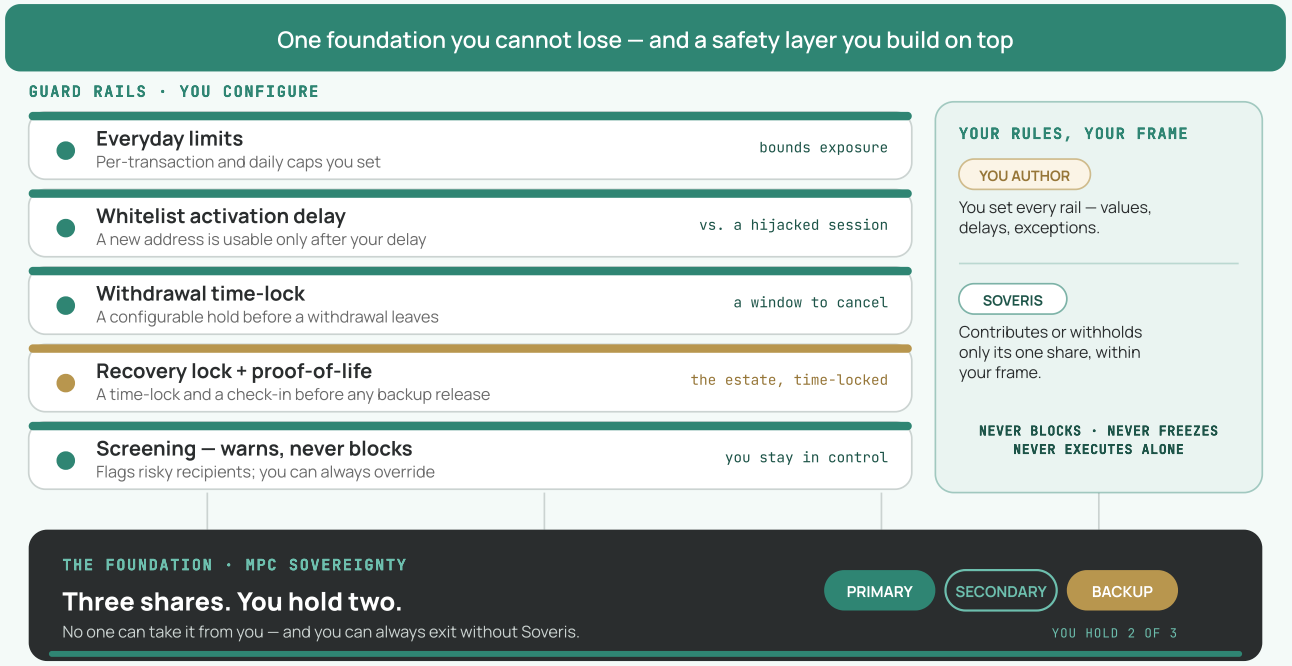
That is the complete surface — both the only thing an attacker would need to find and the only thing you need to safeguard. Because we treat that surface so seriously, Soveris runs a mandatory, gentle cross-check: a quarterly confirmation that you still know your account password, and a yearly attestation — answered simply yes or no, without ever typing it — that you can still retrieve your Recovery Passphrase from wherever you keep it. The purpose is twofold. First, it makes sure that if you ever quietly lose one of the two secrets, it is noticed and repaired while the other is still available to fix it — long before it could become the one situation no one can recover from. Second, the same routine check-in is your *sign of life*: it is the liveness signal that the inheritance and incapacity guard rails (Section 4) listen for, so that those protections only ever engage after a genuine, sustained silence.

4 The Guard Rails: Your Configurable Safety Layer

The foundation in Section 2 decides what is *structurally* possible: Soveris can never move your assets, and you can always act and exit. That guarantee never changes. But a foundation that cannot betray you is only half of what holding real wealth demands. The other half is everyday safety — protection against theft, coercion, a hijacked session, a fat-finger mistake, a lost phone, a death in the family — without surrendering an ounce of control.

That is what the guard rails are: a layer of protections you build on top of the foundation. Each one is a rule **you** author, and the principle that ties them all together is exact and load-bearing:

> A guard rail can only ever change **whether Soveris's single share joins a transaction you have started.** It can never let Soveris act on its own, it can never block, freeze, reverse, or seize, and it can never close the door you hold open with PRIMARY and BACKUP. You set the rule; Soveris honours it by contributing — or withholding — its one co-signing share, within the frame you defined.



MPC plus guard rails. The foundation is a sovereignty guarantee you cannot lose: three shares, two held by you, so no one can take your assets and you can always act and exit. On top sits a safety layer you author — everyday limits, a whitelist activation delay, withdrawal and recovery time-locks with a proof-of-life check-in, and screening that warns rather than blocks. You set every rule; Soveris can only contribute or withhold its single share within the frame you define — it never blocks, freezes, or executes on its own.

This is why convenience and security stop being a trade-off. You dial each protection up or down to taste; the defaults are safe, and a few floors are non-negotiable. The everyday path stays a single biometric gesture, while the limits, delays, and locks you set stand between an attacker and your assets exactly where attacks are fast.

Everyday spending controls — the envelope around routine use

The simplest guard rails draw an envelope around ordinary activity, so a compromised device or a moment of coercion cannot empty everything at once.

- A **per-transaction limit** caps the value of any single transfer. Routine payments clear with a tap; a single send larger than you allow does not go through without deliberate action — and, if you choose, can require a second approval.
- A **daily limit** caps the total value that can leave an everyday wallet within a day. Spend inside it flows freely; anything beyond it waits for the window to reset or for you to raise your own ceiling.

- A **withdrawal time-lock** places a configurable hold on outgoing withdrawals — zero if you want them instant, longer if you want a built-in cooling-off window before a withdrawal completes. You can cancel within the window.

These three are distinct controls doing three different jobs, and they pair naturally with how Soveris separates an everyday spending wallet from the bulk of your holdings: keep a modest amount flowing one-tap, hold the rest behind tighter rails, and the most an attack can reach in the moment is the small envelope you chose to leave open.

Recipient controls — who you can pay, and what we flag

- A **recipient whitelist with an activation delay** governs new destinations. When you add a new address, it becomes usable only after a delay you set — a backstop against an attacker who hijacks a live session and tries to add their own payout address, because by the time the address activates you have seen the change and can cancel it. While a wallet's balance is zero there is nothing to protect, so activation is instant; once it is funded, your delay applies, with escalating warnings as you lower it. Soveris warns; it never blocks; your choice always wins.
- **Screening warns you, it never stops you.** To protect you from unknowingly paying a tainted or sanctioned counterparty, Soveris can screen a destination against known-risk databases and show you a warning and a risk score *before* you send, and it verifies identity and screens against sanctions lists when you open your account. You always see the warning first and you always decide; on your confirmation Soveris contributes its share, and only on your own cancellation does it withhold it. **Soveris never blocks, freezes, or reverses a transaction**, and your exit path is never conditional on our agreement.

The recovery time-lock — protection against coercion

The most important protection against physical coercion is not a stronger password; it is *time*. Releasing your BACKUP share — the recovery path — is gated by a waiting period: **thirty days by default, configurable down to a hard forty-eight-hour floor and up to a ninety-day maximum.** The floor can never be bypassed by any setting, any support action, or any change, and changing the waiting period itself requires re-verification.

The protection, though, is the mechanism, not the number. A coerced recovery is never instant, it announces itself across every channel you have registered, and it remains cancellable for the whole window. The detail that defeats a sophisticated attacker is the asymmetry: **lengthening the waiting period takes effect immediately, but shortening it takes effect only after the current, longer window has already elapsed.** So an attacker who has seized your accounts cannot simply dial the lock down to its floor and start recovery against a shrunken window — they remain bound by whatever window you set while free. The Recovery Passphrase is still required to open the record regardless. The result is that there is no fast payoff to coercion, even at the floor.

The proof-of-life check-in — protection through incapacity and inheritance

Some events are not attacks at all: a death, a coma, a stroke, advancing dementia. The hardest design problem in custody is releasing your wealth to the right person at the right time *without* creating a door an attacker could walk through. Soveris solves it with a check-in.

When you open your account you set an **inactivity timer**, measured in months. Any ordinary sign of life — a login, a signature, the routine check-in from Section 3 — resets it. Only if the timer elapses with *no* sign of life does anything begin to move, and even then a generous, multi-channel cooling period runs first, cancellable the entire time; your simple return to activity stops it at once. The same asymmetry as the recovery lock applies — lengthening the timer is immediate, shortening it takes effect only after the current window — so it cannot be collapsed on the spot.

What the timer releases is bounded in advance and by you. For **incapacity**, the legal authority lives in a power of attorney (in Germany, a *Vorsorgevollmacht*) that you deposit when you set up your account, naming the person you trust; the timer is only the agreed condition under which it may be exercised, never a grant of authority by Soveris. The person you name holds your Recovery Passphrase — but never your account password — so neither they nor Soveris is ever sufficient alone, and Soveris co-signs only within the frame you defined in advance, for example withdrawals to destinations you pre-approved.

For **death**, the path is documentary rather than time-based: your heirs are verified through identity checks and standard German succession documents — a death certificate together with a will or a certificate of inheritance — and after a fourteen-day cooling period the heir becomes the account holder on the same wallet, with the same addresses preserved. A death certificate takes precedence over the incapacity track. In every case, the release reissues shares; Soveris never moves your assets and never decides where they go.

Quiet defences — the controls you never have to think about

A final group runs in the background and asks nothing of you.

- **Automatic key refresh.** Roughly every ninety days, and immediately on any security event, the shares are mathematically refreshed. Your address never changes, but a share an attacker may have quietly captured becomes worthless — capping how long any single compromise could ever matter.
- **Per-customer key separation.** Your key material is fully isolated from every other customer's inside the FIPS-certified HSM, which only ever sees its own share. A problem scoped to one customer cannot cascade; there is no pooled key store to breach.
- **Anomaly detection.** Soveris watches for unusual patterns — velocity, geography, behaviour — and notifies you. It surfaces information and can prompt a review; it never, on its own, stops an action you have authorised.
- **Multi-approval.** For the highest-stakes actions — a large transaction, a change to your whitelist — you can require a second approval before Soveris will contribute its share, so no single moment and no single device can authorise them alone.

5 Built for the Hard Days, Not Just the Easy Ones

A custody system is only as good as its worst day. Section 4 set out the mechanisms; here is how they play out as the real-life events an advisor or attorney can follow — each with a defined path.

A note on how all of these work cryptographically: recovery, inheritance, and incapacity reissue shares rather than moving assets. The technical operation re-creates fresh shares of the *same* underlying key, so **your wallet address is preserved, no on-chain transfer takes place, and no gas is spent.** A full new-key

generation, with assets migrated to a new address, is reserved only for a confirmed compromise. In every flow below, Soveris contributes its share to an action you — or your lawfully established successor — have initiated. Soveris never moves your assets on its own.

EVERY LIFE EVENT HAS A DEFINED PATH

New phone, password known	Restored in under a minute — backup untouched	
Password forgotten	Recover via your BACKUP, behind the recovery time-lock	
Death	Your heir becomes the account holder	address preserved
Incapacity	A power of attorney you deposited in advance releases the mechanism	
Soveris ceases to exist	You self-exit with your own two shares	no Soveris needed

In every path, addresses are preserved and Soveris never moves your assets on its own.

Designed for the hard days. Recovery, inheritance and incapacity reissue shares of the same key — your wallet address is preserved, no on-chain transfer takes place, and Soveris only ever contributes its share to an action you, or your lawful successor, have initiated.

You lose your phone but remember your password

This is the ordinary case described in Section 3: a new device, restored in under a minute, with your BACKUP untouched.

You forget your account password — or your passphrase

Your daily signing never depends on either secret — your phone keeps signing with PRIMARY and SECONDARY — so a forgotten secret is something to repair, not a lockout.

If you lose your **Recovery Passphrase** while your phone and account password still work, you set a new one through a share refresh your phone takes part in, with no time-lock: holding the working device and the password already proves it is you.

Re-establishing a lost **account password** is the more guarded path. Because the password is the anchor that authorises a move to a new device, it runs through your BACKUP — the Knowledge passphrase or the Ownership card — behind the recovery time-lock of Section 4, with re-verification and the un-shortenable waiting window. It is deliberately slower, precisely so that someone who seized your phone cannot quietly reset your password and take over. If your phone is gone too, that same BACKUP path reissues a fresh PRIMARY share to your new device.

A death in the family

When the account holder dies, the wealth does not die with them, and the heirs are not handed a seed phrase and left to cope.

Your heirs are verified as the rightful successors through identity verification and standard German succession documents — a death certificate (Sterbeurkunde) together with a will or a certificate of inheritance (Erbschein), the latter covering cases where no will exists. After a fourteen-day cooling period, the account-holder record is updated, and through a share reissue the heir **becomes the account holder**

on the same wallet, with the same addresses preserved. The heir holds the new PRIMARY share and the BACKUP, and from that point initiates any action themselves. No assets are transferred on-chain by Soveris, and Soveris never directs where assets go.

The design deliberately tolerates the cases real estates encounter. Multiple heirs can be pre-registered with defined splits, so the simultaneous loss of a holder and a co-holder does not collapse the plan. Because the recovery anchor is the Recovery Passphrase in the will and the encrypted record or card in the estate — not a set of living guardians who might die in the same accident — succession does not depend on any one person surviving. And because the heir's task is to install an app, prove their identity, and enter a passphrase or tap a card, no crypto literacy is required of the people you leave behind.

When you are alive but cannot act

Incapacity — a coma, a stroke, advancing dementia — is the case almost no product designs for. Soveris supports it through the proof-of-life check-in of Section 4, resting on a German power of attorney for incapacity (Vorsorgevollmacht) that you deposit when you set up your account, naming the person you trust and the conditions under which they may act.

The legal authority rests entirely in that document, between you and your chosen representative; Soveris operates only the technical release mechanism, within the limits you defined while fully competent. Two evidentiary triggers can release it: the inactivity timer described above, or a document fast-track in which your representative presents the appropriate legal instrument, verified to the same standard as a death certificate. A cooling period and multi-channel warnings apply throughout, and your own return to activity cancels the process at once.

The security model does not bend here. Your representative holds the Recovery Passphrase, handed over privately by you — but never your account password. Soveris releases the encrypted BACKUP only once a trigger fires, and only the passphrase decrypts it; neither alone is sufficient. After release, the BACKUP and Soveris's share together meet the two-of-three threshold, and Soveris co-signs **only within the frame you defined in advance** — for example, withdrawals to destinations you pre-approved. Soveris never holds two shares, never signs alone, and never decides a payout.

6 The Threats, and What Remains

The honest way to present security is not to claim there are no threats, but to walk through the real ones and show what the architecture does about each — including where a residual risk remains. The following is the complete picture; the foundation of Section 2 carries the structural rows, and the guard rails of Section 4 carry the configurable ones.

Threat	How the foundation and guard rails answer it	What remains
Conflict of interest — your assets used to fund a business	No trading desk, no lending book, no staking of your coins. By the architecture, Soveris holds one share of three and cannot move your assets at all — there is nothing to rehypothecate.	Nothing. This failure mode is removed structurally, not promised away.

Threat	How the foundation and guard rails answer it	What remains
The custodian becomes insolvent or disappears	Soveris holding one share cannot strand your assets. Your PRIMARY + BACKUP exit without us, and an insolvency triggers a one-time, offline self-exit tool (Section 7).	You must keep your Recovery Passphrase retrievable; the encrypted backup is useless without it.
Withdrawals are frozen or halted	There is no withdrawal button for us to switch off. You hold two of three shares and broadcast every transaction yourself; Soveris cannot trap your assets.	A determined state actor can still pursue you directly — but the leverage does not sit with Soveris.
Your phone is lost or stolen	Daily signing is gated by biometrics at the secure element, not a passcode, so a thief who watched you type a PIN still cannot sign. Larger holdings sit behind the time-locked recovery a thief cannot reach.	Whatever sits within your everyday spending limits is reachable until you revoke the device, after which a share refresh invalidates it.
An irreversible mistake — wrong address, fat-finger	Per-transaction and daily limits, the withdrawal time-lock, and the recipient-whitelist activation delay each create a moment to catch an error before it leaves.	A send within your own limits, to an address you approved, still goes through; the rails bound mistakes, they do not abolish them.
Coercion or a "wrench attack"	Recovery from the BACKUP is time-locked, so a forced recovery is never instant: it announces itself on every channel and stays cancellable for the entire window, and the asymmetry stops an attacker dialling the lock down. The estate sits behind the lock.	An everyday in-limit amount is still reachable under live duress, and cancellation depends on a warning reaching someone able to act. The lock protects the estate, not the spending wallet — by design.
A hijacked session adds its own withdrawal address	The recipient-whitelist activation delay makes a newly added address unusable until your delay elapses, by which point you have been notified and can cancel.	A first-time, clean-looking address you are deceived into whitelisting and waiting out can still be approved by you — mitigated, not eliminated.
SIM-swap or account takeover	Your account password is the cryptographic anchor, not an SMS code; the recommended configuration uses an authenticator app (TOTP) plus biometrics. A full takeover only lets an attacker *request* recovery — which triggers the time-lock and notifies you everywhere.	A configuration that relies on SMS-based authentication is held to a lower balance ceiling for exactly this reason.
A Soveris insider	One share cannot sign. No employee, at any level of access, can produce a signature alone; per-customer separation and multi-approval add further barriers.	An attacker would still need to independently compromise a second share that only you hold.
A breach of Soveris systems	There is no complete key anywhere to steal. A breach yields a single share — useless on its own. Per-customer separation and the ninety-day refresh contain the blast radius.	An attacker would still need a second, independently secured share.

Threat	How the foundation and guard rails answer it	What remains
A court order served on Soveris	An order compelling Soveris's share compels one share, which alone cannot sign or move assets. Soveris is not in a position to hand the assets over.	A determined state actor can still pursue you directly; Soveris is not where the leverage sits.
A share quietly compromised over years	Automatic ninety-day refresh, plus event-triggered refresh, invalidates old shares while preserving your address.	It narrows the exposure to a single refresh cycle rather than eliminating it: a share captured *and* paired with a second within one window could still matter.
A lost factor or dead device	You never handle a raw seed. A lost phone is restored in under a minute; a lost factor is re-derived from the BACKUP.	Losing one factor is survivable only while the other remains retrievable — which the periodic cross-check (Section 3) exists to ensure. Total loss of every path is covered in Section 9.
A fraudulent inheritance claim	Heirs are pre-registered, matched by identity at succession, verified against multiple official documents, and held through a fourteen-day cooling period before anything changes.	Standard estate-fraud vectors are bounded by multi-document verification and pre-registration, not eliminated.
A compromised phone operating system	A state-actor-grade device implant is outside the normal customer threat model; it is partly addressed by the Ownership BACKUP and the recovery time-lock.	A fully compromised device during in-limit daily spending is exposed. We state this plainly.
A poisoned or swapped destination address	Screening warns before you send to a flagged address — you always decide whether to proceed; the recipient whitelist with its activation delay blunts address-swap attacks.	A first-time, clean-looking attacker address can still be approved by you — mitigated, not eliminated.

For the two controls most easily confused — the recovery time-lock and the whitelist-activation delay — and for the third time-based protection, the withdrawal hold, see Section 4: three different time-based protections doing three different jobs.

7 Independence by Design

The deepest fear in custody is the counterparty fear: *what if the institution I rely on turns against me, or simply disappears?* Soveris answers it not with a reassurance but with a property of the system.

You can always leave

Leaving Soveris is not a courtesy we extend; it is a built-in cryptographic capability. Your two shares — PRIMARY on your phone and your BACKUP — are sufficient on their own to sign a transaction and move your assets to any wallet you choose. No cooperation from Soveris is required, and none can be withheld. There is no vendor lock-in anywhere in the cryptographic anchor; every external component the system uses is substitutable.

If Soveris disappeared tomorrow

If Soveris became insolvent, your assets would not. By default, Soveris stores the single encrypted copy of your backup, released only under strict verification and the recovery time-lock — an anti-theft posture, not a dependency. To make the exit guarantee hold even in that event, Soveris maintains an emergency plan: should the company fail, every customer is sent their own encrypted backup together with a one-time, fully offline, open-source self-exit tool, delivered both in the app and on a publicly mirrored repository.

The tool holds no keys. You run it offline, decrypt your backup with your own Recovery Passphrase, and use your PRIMARY and BACKUP shares to sign an exit and broadcast it through any channel you like. The released backup is useless without your passphrase, so sending it to you adds no risk. In this scenario Soveris contributes no share, signs nothing, and moves nothing. You are the sole actor — exactly as on every other day.

This is the practical meaning of self-sovereignty: the part of the system you cannot personally inspect — our servers, our HSM — is also the part you do not need in order to recover your own assets.

---

8 Where Soveris Stands in Law

Because the wallet is governed by a two-of-three threshold scheme in which Soveris holds only a single co-signing share — never a complete key, never a quorum — Soveris cannot move your assets or reconstruct a key on its own, and you alone initiate and broadcast every transaction. Our considered assessment of this architecture is that Soveris acts as a non-custodial software and MPC-infrastructure provider rather than a crypto-asset custodian, and on that assessment would not be carrying on the regulated activity of crypto-custody as defined under MiCA (Regulation (EU) 2023/1114, Article 3(1)) — in Germany supervised under the Kryptomärkteaufsichtsgesetz (KMAG). We state this as a position grounded in the structure described above, which we are confirming with qualified legal counsel ahead of commercial launch.

This paper is provided for information only. It is not legal, tax, financial, or investment advice, and not an offer of any product or service; Soveris's regulatory position is a considered assessment of the architecture described here, being confirmed with qualified counsel ahead of launch.

---

9 Honest Limits

A document that names its own limits is one you can trust on the claims it does make. Here, plainly, is what Soveris cannot protect you from.

If you lose both of your secrets, no one can recover your assets. The only irrecoverable state in the entire system is the loss of *both* the account password and the Recovery Passphrase at once. Losing one is always survivable — the surviving secret re-establishes the lost one. Losing both leaves no path, for anyone, including Soveris. This is the necessary price of genuine sovereignty: the same property that makes us incapable of betraying you also makes us incapable of overriding a total loss. We make that outcome as unlikely as care and good design allow — the multiple backup paths, and the mandatory periodic cross-check described in Section 3, are built precisely to catch a single loss before it becomes a double one — but we do not pretend it is impossible.

A fully compromised device, during everyday spending, is exposed. A state-actor-grade implant on your phone is outside the normal threat model, and it is partly addressed by the Ownership BACKUP and the recovery time-lock. But while your device is fully owned by an attacker, amounts within your everyday spending limits are reachable. The estate behind the time-lock is not — but the spending wallet is.

A coerced everyday amount remains possible. The recovery time-lock is built to protect the bulk of your wealth from coercion, and it does. But by design it protects the *estate*, not the spending wallet. An attacker applying live, physical pressure can still reach an in-limit daily amount. We would rather tell you exactly where the protection begins and ends than imply a guarantee we cannot keep.

Two of these three limits shrink with how you configure the system: keep your everyday spending wallet modest, hold larger balances behind the time-locked estate, and the bulk of your wealth stays beyond both a compromised device and a coerced reach.

We are aware, too, that after any incident some will say "Soveris held the keys," when Soveris held one share of three and could not have signed anything alone. We would rather state the architecture precisely, here and in advance, than let a convenient shorthand stand in for the truth.

We cannot betray you, because we cannot act alone. Everything else in this paper is the detail of that one sentence.