SOVERIS

SOUVERÄNE VERWAHRUNG

WHITEPAPER · 2026

Souveränität, von Grund auf.

Wie ein Fundament, das dich nicht verraten kann, und Leitplanken, die du selbst bestimmst, dich erhebliche digitale Vermögenswerte halten lassen — ohne die Interessenkonflikte einer Börse und ohne die Zerbrechlichkeit der reinen Self-Custody. In der Architektur angelegt, nicht vertraglich versprochen.

Pure Souveränität. Null Interessenkonflikte. Volle Kontrolle.

Version 1.0 — Juni 2026
soveris.de
Informativ. Keine Rechts- oder Finanzberatung.

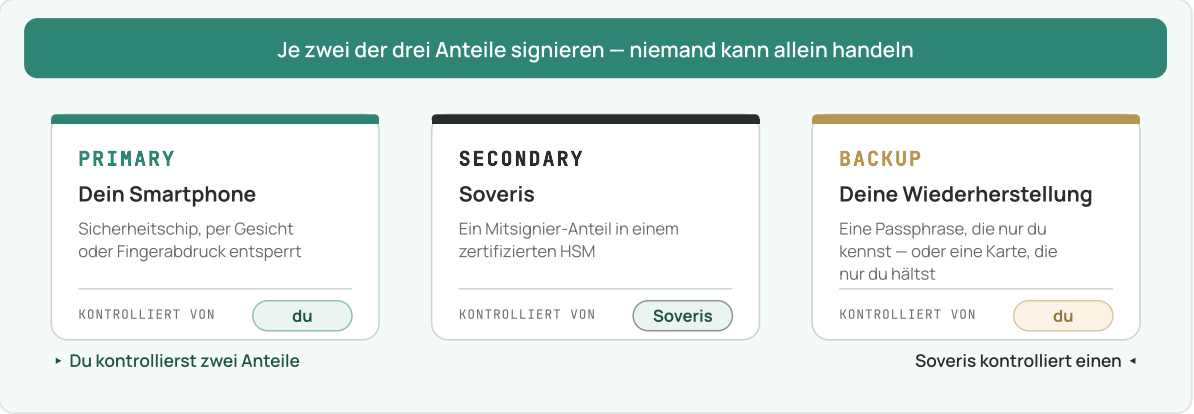
Niemand nimmt es dir — und du verlierst es nicht selbst.

Digitales Vermögen kann man auf genau zwei Arten verlieren: Jemand nimmt es dir – oder du verlierst es selbst. Fast jedes Produkt, das je gebaut wurde, schützt vor dem einen, indem es dich dem anderen aussetzt.

Am einen Ende stehen Börsen und Verwahrer. Sie halten dein Vermögen – und handeln, verleihen oder verpfänden es nicht selten, um das eigene Geschäft zu finanzieren. Du wirst zum ungesicherten Gläubiger, deine Auszahlung kann ausgesetzt werden, und eine einzige Insolvenz oder ein einziger Einbruch kann alles auslöschen. Am anderen Ende steht die reine Eigenverwahrung. Niemand kann dir hier etwas nehmen – doch eine verlorene Seed Phrase, ein plötzlicher Tod ohne geregelte Nachfolge oder ein Moment körperlichen Zwangs löscht alles ebenso vollständig aus. Vom anspruchsvollen Anleger wurde bislang verlangt, sich zu entscheiden, auf welche Weise er verlieren will.

Soveris ist als die eine Position gebaut, die keinem der beiden Enden ausgesetzt ist. Nicht durch ein besseres Versprechen, eine größere Bilanz oder eine Lizenz – sondern durch eine einzige strukturelle Entscheidung und eine Schutzschicht, die du darauf aufbaust.

Deine Wallet ist durch drei unabhängige Schlüssel-Anteile geschützt. Je zwei davon genügen gemeinsam, um eine Transaktion freizugeben. Keine einzelne Partei hält je genug, um allein zu handeln. Zwei der drei Anteile hältst du selbst: einen in der sicheren Hardware deines Telefons, geschützt durch Fingerabdruck oder Gesicht; einen als persönliche Sicherung, über die du allein verfügst. Den dritten hält Soveris in einem Hardware-Sicherheitsmodul. Der vollständige Signaturschlüssel entsteht nirgends – auf keinem Gerät, in keinem Moment, auch nicht während du signierst.



Aus dieser einen Tatsache folgt alles Weitere:

- **Soveris kann nicht allein handeln.** Ein Anteil von dreien kann keine Signatur erzeugen – wir können nicht ohne dich handeln. Das ist keine Richtlinie, an die wir uns zu halten versprechen, sondern eine strukturelle Eigenschaft des Schwellenschemas.
- **Du kannst jederzeit gehen.** Deine zwei Anteile bewegen dein Vermögen in jede Wallet deiner Wahl, ohne jede Mitwirkung von Soveris – selbst wenn es Soveris morgen nicht mehr gäbe.
- **Ein verlorenes Telefon ist kein verlorenes Vermögen.** Ein neues Gerät ist in Minuten wiederhergestellt, nicht in Tagen, deine Sicherung bleibt dabei unberührt. Für die schweren Fälle – Tod, Handlungsunfähigkeit, eine verlorene Passphrase – gibt es jeweils einen definierten, für Anwälte nachvollziehbaren Weg.
- **Dein Nachlass ist geregelt.** Nach deutschem Erbrecht, dem Sitzrecht von Soveris, werden deine Erben über ein definiertes Nachfolgeverfahren zum Kontoinhaber. Keine Seed Phrase, die über den Küchentisch gereicht wird; keine Krypto-Kenntnisse, die du den Hinterbliebenen abverlangst.
- **Ein Interessenkonflikt ist ausgeschlossen.** Kein Handelstisch, kein Verleihbuch, kein Staking deiner Coins – und durch die Architektur selbst kann Soveris dein Vermögen nicht bewegen, um daraus Einnahmen zu erzielen. Der Gleichlauf der Interessen ist strukturell, nicht versprochen.

Dieses Fundament ist nur die Hälfte des Entwurfs. Auf der Grundlage zwei von drei liegt eine Schicht aus *Leitplanken*, die du selbst konfigurierst: eine Obergrenze für das, was eine einzelne Transaktion und ein ganzer Tag bewegen darf, eine Sperrfrist, bevor ein neu hinzugefügter Empfänger bezahlt werden kann, eine Sperrfrist für Auszahlungen, eine Zeitsperre für die Freigabe deiner Sicherung, die Zwang ins Leere laufen lässt, und ein Lebenszeichen-Mechanismus, der dein Vermögen sicher durch Handlungsunfähigkeit und Erbfall trägt. Das Fundament macht Soveris außerstande, dich zu verraten; die Leitplanken machen den alltäglichen Umgang mit deinem eigenen Vermögen zugleich mühelos und sicher – ein einziger biometrischer Handgriff am gewöhnlichen Tag und eine Mauer deines eigenen Entwurfs zwischen einem Angreifer und deinem Nachlass am schlimmsten.

Wie Soveris rechtlich steht. Weil du allein über dein Vermögen verfügst und jede Transaktion allein initiierst und versendest, ist Soveris darauf ausgelegt, als nicht-verwahrender Software- und MPC-Infrastrukturanbieter zu handeln und nicht als Krypto-Verwahrer – eine Einordnung, die wir später in diesem Papier offen darlegen und mit qualifiziertem Rechtsbeistand bestätigen. Soveris stellt das kryptografische Werkzeug bereit; die Souveränität liegt bei dir.

Kein System nimmt jedes Risiko, und dieses Papier wird nicht so tun, als ob. Die folgenden Seiten legen die Architektur dar, die Leitplanken im Detail, die Wege für Wiederherstellung und Nachfolge, die Kryptografie, die rechtliche Einordnung und – offen ausgesprochen – die Grenzen dessen, wovor wir dich schützen können.

1 Das Dilemma der Verwahrung

Frag jemanden, der lange genug digitales Vermögen gehalten hat, was ihn nachts wachhält, und du hörst eine von zwei Sorgen. Entweder *jemand nimmt es mir* – die Börse bricht zusammen, der Verwahrer verleiht die Coins, der Auszahlungsknopf reagiert nicht mehr. Oder *ich verliere es selbst* – die Wiederherstellungsphrase ist verlegt, der Inhaber stirbt und das Vermögen stirbt mit ihm, oder ein Dieb an der Tür erzwingt in Sekunden eine Überweisung.

Das sind nicht zwei Spielarten desselben Risikos. Sie ziehen in entgegengesetzte Richtungen, und genau darin liegt der Kern des Problems.

Wer sein Vermögen einem Verwahrer übergibt, ist vor sich selbst geschützt. Einen Schlüssel, den du nie gehalten hast, kannst du nicht verlegen; vergisst du dein Passwort, setzt der Verwahrer es zurück. Doch du hast dir eine Gegenpartei eingehandelt. Das Geschäft des Verwahrers kann darauf beruhen, dein Vermögen zu nutzen – es zu handeln, zu verleihen, zu verpfänden. Scheitert er, stehst du in einer Reihe mit allen anderen Gläubigern. Die Zusammenbrüche von Verwahrern der vergangenen Jahre waren keine exotischen Ausfälle; sie waren die absehbare Folge davon, einer Partei zugleich das Vermögen und den Anreiz zu überlassen, es zu gebrauchen.

Wer die volle Eigenverwahrung wählt, beseitigt die Gegenpartei vollständig. Niemand kann dein Vermögen einfrieren, verleihen oder über einen gegen einen Dritten gerichteten Gerichtsbeschluss pfänden. Doch jeder Fehler gehört nun dir allein. Eine verlorene Sicherung ist endgültig. Ein Tod ohne Nachfolgeplan löscht den Nachlass. Ein Zwangsangriff gelingt in der Zeit, die das Vorlesen einer Phrase braucht, weil nichts zwischen der Drohung und der Überweisung steht.

Soveris ist so gebaut, dass es an dem einen Punkt liegt, der keinem der beiden Enden ausgesetzt ist.

Verlust ist ein Spektrum. Jedes andere Produkt optimiert ein Ende und versagt am anderen. Die 2-von-3-Teilung trennt „wer es bewegen kann" von „wer es wiederherstellen kann" — Soveris ist keinem der beiden Versagensmuster ausgesetzt.

Jedes Produkt ist ein Punkt auf dieser Linie. Bewegst du dich zum Schutz vor Diebstahl hin, näherst du dich dem Selbstverlust; bewegst du dich zum Schutz vor Selbstverlust hin, kehrst du zur Gegenpartei zurück. Andere Dienste, die Schlüssel mit ihren Kunden teilen, haben die Mitte zwischen beiden Enden ernsthaft besetzt – und sind dabei weit gekommen. Doch die Mitte, die sie erreichen, bleibt ein Kompromiss: weitgehend nur Bitcoin, oft technisches Können vom Inhaber und seinen Erben verlangend und selten um europäisches Recht oder europäische Nachlässe herum gebaut.

Soveris wurde gebaut, um einen einzigen Punkt auf dieser Linie zu besetzen, der keinem der beiden Enden ausgesetzt ist. Der Mechanismus, der das möglich macht, ist Gegenstand des nächsten Abschnitts.

2 Das Fundament: So arbeitet Soveris

Der gesamte Entwurf ruht auf einem einzigen Gedanken, deshalb lohnt es sich, ihn langsam auszusprechen.

Deine Wallet wird von **drei unabhängigen Schlüssel-Anteilen** bestimmt. Kryptografen nennen das Schwellenwert-Kryptografie oder Mehrparteienberechnung – kurz MPC. Eine Transaktion wird freigegeben, wenn **je zwei der drei Anteile** an der Signatur mitwirken. Ein einzelner Anteil genügt nie. Und – das ist das Entscheidende – der vollständige Signaturschlüssel entsteht nirgendwo: nicht auf deinem Telefon, nicht auf unseren Systemen, keinen Augenblick lang während der Signatur. Jeder Anteil ist für sich genommen ein nutzloses Bruchstück.

Die drei Anteile haben unterschiedliche Rollen und unterschiedliche Hüter.

Anteil	Wo er lebt	Was ihn schützt	Wer ihn kontrolliert
PRIMARY	In der sicheren Hardware deines Telefons – der Secure Enclave beim iPhone, StrongBox bei Android	Hardware-Isolation und dein Fingerabdruck oder Gesicht; der Anteil verlässt das Sicherheitselement nie in lesbarer Form	Du
SECONDARY	In einem von Soveris betriebenen Hardware-Sicherheitsmodul (HSM)	Ein FIPS-zertifiziertes HSM, in dem das Schlüsselmaterial jedes Kunden vollständig getrennt gehalten wird	Soveris
BACKUP	Deine Wahl: als *Wissen* (ein verschlüsselter Datensatz, allein mit deiner Wiederherstellungs-Passphrase zu öffnen) oder als *Besitz* (eine physische Karte mit Sicherheitselement, die du behältst)	Wissen: ein Verschlüsselungsverfahren, das deine Passphrase absichtlich viel Arbeitsspeicher verlangen lässt (speicherhart), um Brute-Force teuer zu machen. Besitz: das Sicherheitselement der Karte und ihre PIN	Du

Du hältst immer zwei der drei: PRIMARY auf deinem Telefon und BACKUP, wo immer du es aufbewahrst. Das ist die kryptografische Grundlage für das Wort *souverän*. Drei Aussagen folgen unmittelbar daraus, und das ganze Fundament ist in ihnen enthalten:

- **Soveris allein, mit einem Anteil, kann nicht signieren.** Es ist nicht so, dass wir es nicht wollen – durch den Entwurf des Schwellenschemas kann ein einzelner Anteil von dreien keine Signatur erzeugen. Wir können nicht ohne dich handeln.
- **Du allein, mit PRIMARY und BACKUP, kannst signieren – und jederzeit gehen**, ganz ohne Mitwirkung von Soveris.
- **Du und Soveris gemeinsam, mit PRIMARY und SECONDARY, bilden das Alltags-Quorum**, das deine täglichen Transaktionen signiert.

WAS JEDE KOMBINATION KANN

Soveris allein 1 Anteil	Kann nicht signieren — mathematisch unmöglich
Du allein PRIMARY + BACKUP	Kann signieren und Soveris jederzeit ganz verlassen
Du + Soveris PRIMARY + SECONDARY	Das normale Alltags-Quorum mit einem Fingertipp

Drei Kombinationen, eine Garantie. Nur Kombinationen, die dich einschließen, können signieren. Soveris ist allein nie ausreichend.

Durchgängig gilt ein Grundsatz ohne Ausnahme: **du initiierst jede Transaktion, und du allein sendest sie ins Netzwerk.** Soveris steuert seinen Mitsignier-Anteil erst bei, wenn du eine von dir begonnene Handlung freigibst. Soveris beginnt nie eine Transaktion in deinem Namen, und Soveris versendet nie. Ohne dein Zutun geschieht nichts.

Die Kryptografie, klar gesagt

Soveris nutzt moderne, peer-reviewte Schwellenwert-Signaturverfahren, bewusst so gewählt, dass sie ältere Verfahren mit bekannten Schwachstellenklassen meiden. Die Signaturen, die das System erzeugt, sind gewöhnliche Signaturen auf der Blockchain – nicht von denen einer Ein-Schlüssel-Wallet zu unterscheiden und über viele Blockchains hinweg unterstützt, nicht nur über eine.

Der PRIMARY-Anteil auf dem Gerät liegt im Sicherheitselement des Telefons, durch Biometrie gesichert und vom Betriebssystem verwaltet; er wird nie in lesbarer Form ausgegeben. Ein Punkt verdient Genauigkeit, denn technische Leser werden ihn prüfen: **dein Fingerabdruck oder dein Gesicht wird nie genutzt, um einen Verschlüsselungsschlüssel abzuleiten.** Biometrie ist eine Bequemlichkeit des Betriebssystems, die den Anteil auf dem Gerät für das tägliche Signieren entsperrt. Der tragbare kryptografische Anker ist dein Konto-Passwort, nie deine Biometrie – diese ist an ein Gerät gebunden und kann nicht mitreisen.

Das HSM von Soveris ist FIPS-zertifiziert, mit einem geplanten Weg hin zu einem dedizierten Modul nach FIPS 140-3 Level 3. Das Schlüsselmaterial jedes Kunden ist von dem jedes anderen vollständig getrennt und mit AES-256-GCM umschlossen. Das HSM sieht stets nur seinen eigenen SECONDARY-Anteil und den gemeinsamen öffentlichen Schlüssel; es sieht weder PRIMARY noch BACKUP.

Das BACKUP in der Form *Wissen* ist mit der authentifizierten Verschlüsselung XChaCha20-Poly1305 gesichert, unter einem Schlüssel, der aus deiner Wiederherstellungs-Passphrase mit Argon2id abgeleitet wird – einem Verfahren, das absichtlich viel Arbeitsspeicher verlangt (speicherhart), eigens gewählt, um Brute-Force teuer zu machen, selbst gegen spezialisierte Hardware. Soveris speichert nur den entstehenden verschlüsselten Text und einen nicht-geheimen Zufallswert; **Soveris kann den Schlüssel nicht ableiten und den Datensatz nicht entschlüsseln.** Jeder verschlüsselte Datensatz ist kryptografisch an seine Version und an den Fingerabdruck des öffentlichen Schlüssels deiner Wallet gebunden, was Wiedereinspiel-, Rückroll- und Austauschangriffe verhindert.

Etwa alle neunzig Tage – und sofort bei jedem Sicherheitsereignis – werden die Anteile mathematisch erneuert, dein Telefon wirkt am regelmäßigen Zyklus mit. Der öffentliche Schlüssel und deine Wallet-Adresse bleiben unverändert erhalten, doch die früheren Anteile werden kryptografisch ungültig, selbst

wenn ein Angreifer stillschweigend einen behalten hätte. Das begrenzt das Zeitfenster, in dem ein einzelner kompromittierter Anteil überhaupt etwas bedeuten könnte.

Schließlich musst du uns nicht aufs Wort glauben, was wir für dich halten. Jeder Kunde hat eigene Adressen auf der Blockchain, von jedem, jederzeit, in jedem öffentlichen Verzeichnis der Blockchain (Block-Explorer) prüfbar. Wir nennen das *Nachweis der Bestände*, und er ist stärker als der periodische *Reservennachweis*, den eine Börse veröffentlichen mag: deiner ist fortlaufend, ohne Erlaubnis einsehbar und allein dir zugeordnet, kein gepoolter Schnappschuss, dem du vertrauen musst.

Nirgends in diesem Bild sitzt eine Abhängigkeit von einem Anbieter. Jede externe Komponente ist austauschbar; die kryptografische Garantie, dass du jederzeit aussteigen kannst, hängt an keinem einzelnen Lieferanten.

---

3 Ein Tag mit Soveris

Souveränität sollte sich nicht wie Disziplin anfühlen. Im Alltag fühlt sie sich an, als entsperrtest du dein Telefon.

Du öffnest die App und bereitest eine Transaktion vor – ein Betrag, ein Empfänger. Du bestätigst mit Fingerabdruck oder Gesicht. Hinter dieser einen Geste führen der PRIMARY-Anteil deines Telefons und der SECONDARY-Anteil im HSM von Soveris einen kurzen Signatur-Austausch, und die fertige Signatur entsteht auf deinem Gerät. Deine App sendet die signierte Transaktion dann ins Netzwerk – über ein öffentliches Relais, deinen eigenen Knoten (Node) oder jeden Weg, den du vorziehst. Keine Seed Phrase zu tippen, kein Passwort beim Signieren, kein zweites Hardware-Gerät zu suchen. Es ist dieselbe Geste, die du längst für eine Banking-App nutzt.

Eine ganz normale Signatur. Ein Fingertipp — keine Seed-Phrase, kein Hardware-Ritual. Soveris steuert seinen Mitsignier-Anteil erst bei, nachdem du freigegeben hast, und veröffentlicht nie selbst: Du hältst und sendest die fertig signierte Transaktion.

Genau gesagt, wer was tut: du initiierst die Transaktion, du gibst sie biometrisch frei, und dein Gerät hält und versendet die fertig signierte Transaktion. Soveris steuert einen Mitsignier-Anteil bei, wenn du darum bittest, und sonst nichts.

Wenn du das Telefon wechselst

Ein neues Telefon ist das häufigste Ereignis im echten Leben, und es ist bewusst undramatisch. Du installierst die App und meldest dich mit deinem Konto-Passwort an, dann hinterlegst du erneut deine Biometrie. Die verschlüsselte Sicherung deines PRIMARY-Anteils wird abgerufen und lokal auf deinem Gerät mit deinem Konto-Passwort entschlüsselt – das nie zu Soveris gelangt. Der Anteil wird anschließend neu im Sicherheitselement deines neuen Telefons versiegelt. Dein BACKUP-Anteil bleibt unberührt. Der Zielwert liegt unter einer Minute.

Die zwei Dinge zum Merken

Für dein ganzes Leben mit Soveris hältst du genau zwei Geheimnisse. Alles Übrige – Biometrie, App-Sitzungen, Geräte-Kopplungen – ist Komfort, den jedes neue Gerät wiederaufbauen kann.

- Ein **Konto-Passwort**, wie jede andere Anmeldung. Es darf in einem Passwort-Manager liegen, und es ist das Geheimnis, das den Wechsel auf ein neues Gerät verankert.
- Eine **Wiederherstellungs-Passphrase**, einmal bei der Anmeldung notiert und dort verwahrt, wo du wichtige Dokumente aufbewahrst – bei deinem Testament, im Safe oder bei deinem Anwalt. Du tippst sie selten bis nie; sie existiert für die Ausnahmefälle.

Das ist die vollständige Angriffsfläche – zugleich das Einzige, was ein Angreifer finden müsste, und das Einzige, was du sichern musst. Weil wir diese Fläche so ernst nehmen, führt Soveris eine verpflichtende, behutsame Gegenprobe: ein vierteljährliches Bestätigen, dass du dein Konto-Passwort noch weißt, und eine jährliche Versicherung – schlicht mit Ja oder Nein beantwortet, ohne sie je zu tippen –, dass du deine Wiederherstellungs-Passphrase noch dort findest, wo du sie aufbewahrst. Der Zweck ist ein doppelter. Erstens stellt er sicher, dass ein stiller Verlust eines der zwei Geheimnisse bemerkt und behoben wird, solange das andere noch da ist, um es zu heilen – lange bevor daraus die eine Lage werden könnte, aus der niemand mehr zurückführt. Zweitens ist dieselbe regelmäßige Gegenprobe dein *Lebenszeichen*: sie ist das Lebenssignal, auf das die Leitplanken für Erbfall und Handlungsunfähigkeit (Abschnitt 4) hören, damit diese Schutzmechanismen erst nach einer echten, anhaltenden Stille überhaupt anspringen.

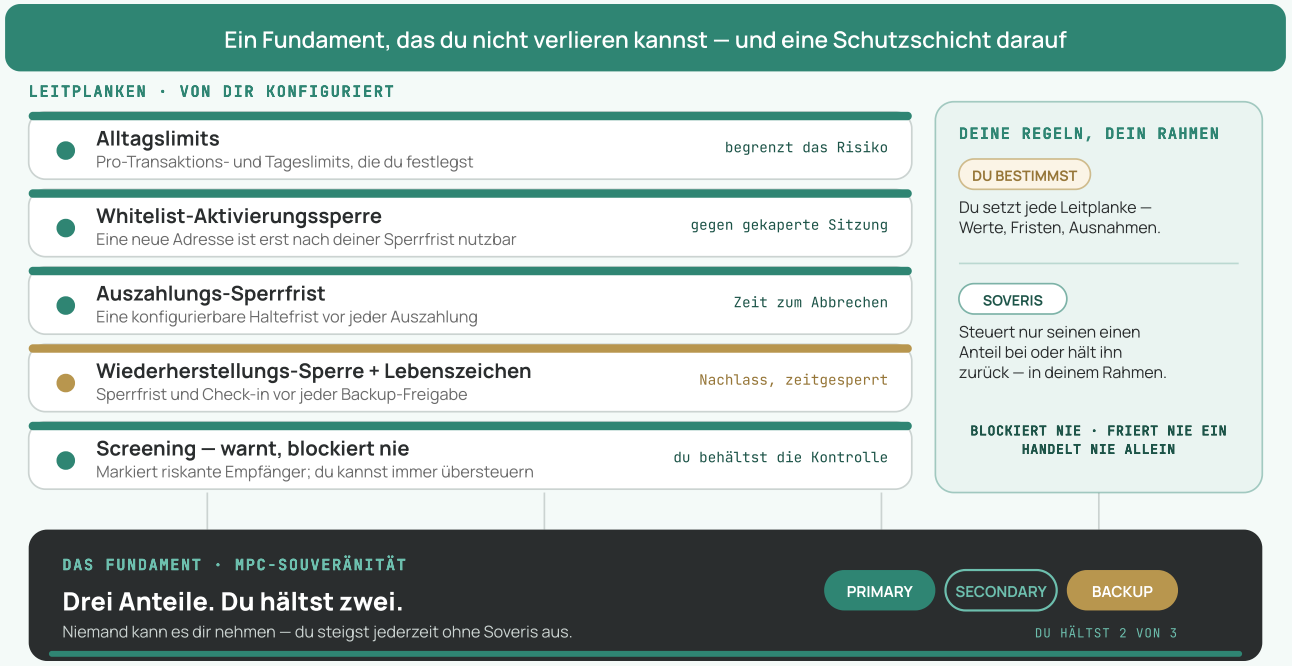
---

4 Die Leitplanken: Deine konfigurierbare Schutzschicht

Das Fundament aus Abschnitt 2 entscheidet, was *strukturell* möglich ist: Soveris kann dein Vermögen nie aus eigener Kraft bewegen, und du kannst immer handeln und aussteigen. Diese Garantie ändert sich nie. Doch ein Fundament, das dich nicht verraten kann, ist nur die Hälfte dessen, was echtes Vermögen verlangt. Die andere Hälfte ist die alltägliche Sicherheit – Schutz gegen Diebstahl, Zwang, eine gekaperte Sitzung, einen Vertipper, ein verlorenes Telefon, einen Todesfall in der Familie – ohne dass du auch nur ein Gramm Kontrolle abgibst.

Genau das sind die Leitplanken: eine Schicht aus Schutzmechanismen, die du auf dem Fundament aufbaust. Jede einzelne ist eine Regel, die **du** verfasst, und das Prinzip, das sie alle zusammenhält, ist genau und tragend:

> Eine Leitplanke kann immer nur ändern, **ob der einzelne Anteil von Soveris einer Transaktion beitritt, die du begonnen hast.** Sie kann Soveris nie aus eigenem Antrieb handeln lassen, sie kann nie blockieren, einfrieren, umkehren oder pfänden, und sie kann nie die Tür schließen, die du mit PRIMARY und BACKUP offen hältst. Du setzt die Regel; Soveris wahrt sie, indem es seinen einen Mitsignier-Anteil beisteuert – oder zurückhält –, innerhalb des Rahmens, den du gesetzt hast.



MPC plus Leitplanken. Das Fundament ist eine Souveränitäts-Garantie, die du nicht verlieren kannst: drei Anteile, zwei davon hältst du — niemand kann dir deine Werte nehmen, und du kannst jederzeit handeln und aussteigen. Darauf eine Schutzschicht, die du selbst bestimmst — Alltagslimits, eine Whitelist-Aktivierungssperre, Auszahlungs- und Wiederherstellungs-Sperrfristen mit Lebenszeichen-Check-in sowie ein Screening, das warnt statt zu blockieren. Du setzt jede Regel; Soveris steuert nur seinen einen Anteil bei oder hält ihn zurück — in deinem Rahmen. Es blockiert nie, friert nie ein und handelt nie allein.

Deshalb hören Komfort und Sicherheit auf, ein Tauschgeschäft zu sein. Du drehst jeden Schutz nach deinem Geschmack auf oder ab; die Voreinstellungen sind sicher, und einige Untergrenzen sind nicht verhandelbar. Der Alltagsweg bleibt ein einziger biometrischer Handgriff, während die Grenzen, Sperrfristen und Sperren, die du setzt, genau dort zwischen einem Angreifer und deinem Vermögen stehen, wo Angriffe schnell sind.

Alltagslimits – der Rahmen um die gewöhnliche Nutzung

Die einfachsten Leitplanken ziehen einen Rahmen um die gewöhnliche Aktivität, damit ein kompromittiertes Gerät oder ein Moment des Zwangs nicht alles auf einmal leeren kann.

- Ein **Pro-Transaktions-Limit** begrenzt den Wert jeder einzelnen Überweisung. Routinezahlungen gehen mit einem Fingertipp durch; eine einzelne Sendung, die größer ist, als du erlaubst, geht nicht ohne bewusste Handlung durch – und kann, wenn du es so wählst, eine zweite Freigabe verlangen.
- Ein **Tageslimit** begrenzt den Gesamtwert, der eine Alltags-Wallet innerhalb eines Tages verlassen kann. Ausgaben innerhalb dieser Grenze fließen frei; alles darüber wartet, bis das Fenster sich zurücksetzt oder du deine eigene Obergrenze anhebst.
- Eine **Auszahlungs-Sperrfrist** legt eine konfigurierbare Wartezeit über ausgehende Auszahlungen – null, wenn du sie sofort möchtest, länger, wenn du dir vor dem Abschluss einer Auszahlung ein eingebautes Fenster zum Innehalten wünschst. Innerhalb des Fensters kannst du abbrechen.

Das sind drei eigenständige Kontrollen, die drei verschiedene Aufgaben erfüllen, und sie passen natürlich dazu, wie Soveris eine Alltags-Wallet vom Großteil deiner Bestände trennt: lass einen bescheidenen Betrag mit einem Fingertipp fließen, halte den Rest hinter strengeren Leitplanken – und das Höchste, was ein Angriff im Moment erreichen kann, ist der kleine Rahmen, den du bewusst offen gelassen hast.

Empfängerkontrollen – wen du bezahlen kannst, und worauf wir hinweisen

- Eine **Empfänger-Whitelist mit Aktivierungssperre** regelt neue Ziele. Fügst du eine neue Adresse hinzu, wird sie erst nach einer Sperrfrist nutzbar, die du setzt – ein Riegel gegen einen Angreifer, der eine laufende Sitzung kapert und seine eigene Auszahlungsadresse einschmuggeln will, denn bis die Adresse aktiv wird, hast du die Änderung gesehen und kannst sie abbrechen. Solange das Guthaben einer Wallet null ist, gibt es nichts zu schützen, also ist die Aktivierung sofort; sobald sie befüllt ist, greift deine Sperrfrist, mit eskalierenden Warnungen, je weiter du sie senkst. Soveris warnt; es blockiert nie; deine Wahl gewinnt immer.
- **Das Screening warnt dich, es hält dich nie auf.** Um dich davor zu schützen, unwissentlich an eine belastete oder sanktionierte Gegenpartei zu zahlen, kann Soveris ein Ziel gegen Datenbanken bekannter Risiken prüfen und dir eine Warnung samt Risikobewertung zeigen, *bevor* du sendest, und es prüft die Identität und gleicht bei der Aufnahme gegen Sanktionslisten ab. Du siehst stets zuerst die Warnung, und du entscheidest stets; auf deine Bestätigung steuert Soveris seinen Anteil bei, und nur auf deinen eigenen Abbruch hält es ihn zurück. **Soveris blockiert, sperrt oder kehrt nie eine Transaktion um**, und dein Weg zum Ausstieg hängt nie von unserer Zustimmung ab.

Die Wiederherstellungs-Sperrfrist – Schutz gegen Zwang

Der wichtigste Schutz gegen körperlichen Zwang ist kein stärkeres Passwort; es ist *Zeit*. Die Freigabe deines BACKUP-Anteils – der Weg zur Wiederherstellung – ist an eine Wartezeit gebunden: **voreingestellt dreißig Tage, konfigurierbar herunter bis zu einer harten Untergrenze von achtundvierzig Stunden und hinauf bis zu einem Höchstwert von neunzig Tagen.** Die Untergrenze lässt sich durch keine Einstellung, keine Support-Handlung und keine Änderung umgehen, und die Wartezeit selbst zu ändern verlangt eine erneute Verifizierung.

Der Schutz aber liegt im Mechanismus, nicht in der Zahl. Eine erzwungene Wiederherstellung ist nie sofort, sie meldet sich über jeden Kanal, den du hinterlegt hast, und sie bleibt das ganze Fenster über abbrechbar. Das Detail, das einen ausgefeilten Angreifer schlägt, ist die Asymmetrie: **das Verlängern der Wartezeit wirkt sofort, ihr Verkürzen aber erst, nachdem das aktuelle, längere Fenster bereits abgelaufen ist.** Ein Angreifer, der deine Konten an sich gebracht hat, kann die Sperre also nicht einfach auf ihre Untergrenze drehen und die Wiederherstellung gegen ein verkürztes Fenster starten – er bleibt an das Fenster gebunden, das du in Freiheit gesetzt hast. Die Wiederherstellungs-Passphrase ist ohnehin weiter nötig, um den Datensatz zu öffnen. Im Ergebnis gibt es keinen schnellen Ertrag für Zwang, selbst an der Untergrenze.

Das Lebenszeichen – Schutz durch Handlungsunfähigkeit und Erbfall

Manche Ereignisse sind gar keine Angriffe: ein Tod, ein Koma, ein Schlaganfall, fortschreitende Demenz. Das schwierigste Entwurfsproblem in der Verwahrung ist, dein Vermögen zur richtigen Zeit der richtigen Person freizugeben, *ohne* dabei eine Tür zu schaffen, durch die ein Angreifer gehen könnte. Soveris löst es über ein Lebenszeichen.

Wenn du dein Konto einrichtest, setzt du einen **Inaktivitäts-Zähler**, gemessen in Monaten. Jedes gewöhnliche Lebenszeichen – eine Anmeldung, eine Signatur, die regelmäßige Gegenprobe aus Abschnitt 3 – setzt ihn zurück. Erst wenn der Zähler abläuft, *ohne* dass ein Lebenszeichen kommt, beginnt überhaupt etwas sich zu bewegen, und selbst dann läuft zuvor eine großzügige Wartezeit über mehrere

Kanäle, die ganze Zeit abbrechbar; deine schlichte Rückkehr zur Aktivität stoppt sie sofort. Dieselbe Asymmetrie wie bei der Wiederherstellungs-Sperrfrist gilt – den Zähler zu verlängern wirkt sofort, ihn zu verkürzen erst nach dem aktuellen Fenster –, sodass er sich nicht auf der Stelle zusammenstauchen lässt.

Was der Zähler freigibt, ist im Voraus und von dir begrenzt. Für die **Handlungsunfähigkeit** liegt die rechtliche Befugnis in einer Vollmacht (in Deutschland einer *Vorsorgevollmacht*), die du beim Einrichten deines Kontos hinterlegst und in der du die Person deines Vertrauens benennst; der Zähler ist nur die vereinbarte Bedingung, unter der sie ausgeübt werden darf, nie eine Befugnis, die Soveris erteilt. Die von dir benannte Person hält deine Wiederherstellungs-Passphrase – aber nie dein Konto-Passwort –, sodass weder sie noch Soveris je allein genügt, und Soveris signiert nur innerhalb des Rahmens mit, den du im Voraus gesetzt hast, etwa Auszahlungen an Ziele, die du vorab freigegeben hast.

Für den **Tod** ist der Weg dokumentarisch statt zeitbasiert: deine Erben werden über Identitätsprüfungen und übliche deutsche Nachlassdokumente festgestellt – eine Sterbeurkunde zusammen mit einem Testament oder einem Erbschein –, und nach einer Wartefrist von vierzehn Tagen wird der Erbe zum Kontoinhaber auf derselben Wallet, mit denselben erhaltenen Adressen. Eine Sterbeurkunde hat Vorrang vor dem Weg der Handlungsunfähigkeit. In jedem Fall werden bei der Freigabe die Anteile neu ausgegeben; Soveris bewegt dein Vermögen nie und entscheidet nie, wohin es fließt.

Leise Schutzmechanismen – die Kontrollen, an die du nie denken musst

Eine letzte Gruppe läuft im Hintergrund und verlangt dir nichts ab.

- **Automatische Schlüsselerneuerung.** Etwa alle neunzig Tage – und sofort bei jedem Sicherheitsereignis – werden die Anteile mathematisch erneuert. Deine Adresse ändert sich nie, doch ein Anteil, den ein Angreifer stillschweigend erbeutet haben mag, wird wertlos – das begrenzt, wie lange eine einzelne Kompromittierung überhaupt etwas bedeuten könnte.
- **Mandantentrennung.** Dein Schlüsselmaterial ist von dem jedes anderen Kunden vollständig getrennt, innerhalb des FIPS-zertifizierten HSM, das stets nur seinen eigenen Anteil sieht. Ein Problem, das auf einen Kunden begrenzt ist, kann nicht kaskadieren; es gibt keinen gepoolten Schlüsselspeicher, in den man einbrechen könnte.
- **Anomalieerkennung.** Soveris achtet auf ungewöhnliche Muster – Geschwindigkeit, Geografie, Verhalten – und benachrichtigt dich. Es legt Informationen offen und kann eine Überprüfung anstoßen; es hält aus eigenem Antrieb nie eine Handlung auf, die du freigegeben hast.
- **Mehrfachfreigabe.** Für die folgenreichsten Handlungen – eine große Transaktion, eine Änderung an deiner Whitelist – kannst du eine zweite Freigabe verlangen, bevor Soveris seinen Anteil beisteuert, sodass kein einzelner Moment und kein einzelnes Gerät sie allein freigeben kann.

---

5 Gebaut für die schweren Tage

Ein Verwahrsystem ist nur so gut wie sein schlimmster Tag. Abschnitt 4 hat die Mechanismen dargelegt; hier ist, wie sie sich als die Ereignisse des echten Lebens entfalten, denen ein Berater oder Anwalt folgen kann – jedes mit einem definierten Weg.

Eine Anmerkung dazu, wie all das kryptografisch funktioniert: Bei Wiederherstellung, Vererbung und Handlungsunfähigkeit werden die Anteile neu ausgegeben, statt Vermögen zu bewegen. Der technische Vorgang erzeugt frische Anteile *desselben* zugrunde liegenden Schlüssels, deshalb bleibt **deine Wallet-Adresse erhalten, auf der Blockchain wird nichts übertragen, und es fallen keine Netzgebühren an.**

Eine vollständige Neuerzeugung des Schlüssels, mit Verschiebung des Vermögens auf eine neue Adresse, ist allein einer bestätigten Kompromittierung vorbehalten. In jedem der folgenden Abläufe steuert Soveris seinen Anteil zu einer Handlung bei, die du – oder dein rechtmäßig festgestellter Nachfolger – begonnen hast. Soveris bewegt dein Vermögen nie aus eigenem Antrieb.

JEDES LEBENSEREIGNIS HAT EINEN DEFINIERTEN WEG

Neues Smartphone, Passwort bekannt	In unter einer Minute wiederhergestellt — Backup unberührt	
Passwort vergessen	Wiederherstellung über dein BACKUP, hinter der Wiederherstellungs-Sperrfrist	
Todesfall	Deine Erben werden Account-Inhaber	Adresse bleibt erhalten
Handlungsunfähigkeit	Eine im Voraus hinterlegte Vorsorgevollmacht löst den Mechanismus aus	
Soveris existiert nicht mehr	Du steigst mit deinen eigenen zwei Anteilen selbst aus	ohne Soveris

Auf jedem Weg bleiben die Adressen erhalten, und Soveris bewegt deine Werte nie von sich aus.

Für die schweren Tage gebaut. Wiederherstellung, Erbfall und Handlungsunfähigkeit erzeugen neue Anteile desselben Schlüssels — deine Wallet-Adresse bleibt erhalten, auf der Blockchain wird nichts übertragen, und Soveris steuert seinen Anteil nur zu einer Aktion bei, die du oder dein rechtmäßiger Nachfolger gestartet hast.

Du verlierst dein Telefon, weißt aber dein Passwort

Das ist der gewöhnliche Fall aus Abschnitt 3: ein neues Gerät, in unter einer Minute wiederhergestellt, dein BACKUP unberührt.

Du vergisst dein Konto-Passwort – oder deine Passphrase

Dein tägliches Signieren hängt an keinem der beiden Geheimnisse – dein Telefon signiert weiter mit PRIMARY und SECONDARY –, ein vergessenes Geheimnis ist also etwas zu Behebendes, keine Aussperrung.

Verlierst du deine **Wiederherstellungs-Passphrase**, während dein Telefon und dein Konto-Passwort noch funktionieren, vergibst du eine neue über eine Neuausgabe der Anteile, an der dein Telefon mitwirkt – ohne Sperrfrist: das funktionierende Gerät und das Passwort in der Hand beweisen bereits, dass du es bist.

Ein verlorenes **Konto-Passwort** neu aufzusetzen ist der stärker gesicherte Weg. Weil das Passwort der Anker ist, der den Wechsel auf ein neues Gerät freigibt, läuft es über dein BACKUP – die Knowledge-Passphrase oder die Ownership-Karte – hinter der Wiederherstellungs-Sperrfrist aus Abschnitt 4, mit erneuter Verifizierung und dem unverkürzbaren Wartefenster. Er ist bewusst langsamer, eben damit jemand, der dein Telefon an sich gebracht hat, dein Passwort nicht stillschweigend zurücksetzen und dich übernehmen kann. Ist auch dein Telefon fort, gibt derselbe BACKUP-Weg deinem neuen Gerät einen frischen PRIMARY-Anteil aus.

Ein Todesfall in der Familie

Stirbt der Kontoinhaber, stirbt das Vermögen nicht mit ihm, und die Erben bekommen keine Seed Phrase in die Hand gedrückt, mit der sie allein zurechtkommen müssen.

Deine Erben werden über eine Identitätsprüfung und die üblichen deutschen Nachlassdokumente als rechtmäßige Nachfolger festgestellt – eine Sterbeurkunde zusammen mit einem Testament oder einem Erbschein, wobei Letzterer die Fälle ohne Testament abdeckt. Nach einer Wartefrist von vierzehn Tagen wird der Eintrag des Kontoinhabers aktualisiert, und über eine Neuausgabe der Anteile wird der Erbe **zum Kontoinhaber auf derselben Wallet, mit denselben erhaltenen Adressen.** Der Erbe hält den neuen PRIMARY-Anteil und das BACKUP und initiiert von da an jede Handlung selbst. Soveris überträgt nichts auf der Blockchain, und Soveris bestimmt nie, wohin Vermögen fließt.

Der Entwurf duldet bewusst die Fälle, denen echte Nachlässe begegnen. Mehrere Erben lassen sich mit festgelegten Quoten vorab eintragen, sodass der gleichzeitige Verlust eines Inhabers und eines Mitinhabers den Plan nicht zum Einsturz bringt. Weil der Anker der Wiederherstellung die Wiederherstellungs-Passphrase im Testament und der verschlüsselte Datensatz oder die Karte im Nachlass ist – nicht eine Gruppe lebender Vertrauter, die im selben Unglück sterben könnten –, hängt die Nachfolge nicht am Überleben einer einzelnen Person. Und weil die Aufgabe des Erben darin besteht, eine App zu installieren, seine Identität nachzuweisen und eine Passphrase einzugeben oder eine Karte aufzulegen, verlangt sie den Hinterbliebenen keine Krypto-Kenntnisse ab.

Wenn du lebst, aber nicht handeln kannst

Handlungsunfähigkeit – ein Koma, ein Schlaganfall, fortschreitende Demenz – ist der Fall, für den fast kein Produkt entwirft. Soveris trägt ihm über das Lebenszeichen aus Abschnitt 4 Rechnung, das auf einer deutschen Vorsorgevollmacht ruht, die du beim Einrichten deines Kontos hinterlegst und in der du die Person deines Vertrauens benennst und die Bedingungen, unter denen sie handeln darf.

Die rechtliche Befugnis liegt ganz in diesem Dokument, zwischen dir und deinem gewählten Vertreter; Soveris betreibt nur den technischen Freigabe-Mechanismus, in den Grenzen, die du bei voller Geschäftsfähigkeit gesetzt hast. Zwei Nachweis-Auslöser können ihn freigeben: der oben beschriebene Inaktivitäts-Zähler oder ein Dokumenten-Schnellweg, bei dem dein Vertreter das passende Rechtsdokument vorlegt, geprüft nach demselben Maßstab wie eine Sterbeurkunde. Eine Wartefrist und Warnungen über mehrere Kanäle greifen durchgängig, und deine eigene Rückkehr zur Aktivität bricht den Vorgang sofort ab.

Das Sicherheitsmodell biegt hier nicht ab. Dein Vertreter hält die Wiederherstellungs-Passphrase, von dir privat übergeben – aber nie dein Konto-Passwort. Soveris gibt das verschlüsselte BACKUP erst frei, sobald ein Auslöser greift, und allein die Passphrase entschlüsselt es; keines von beiden genügt für sich. Nach der Freigabe erreichen das BACKUP und der Anteil von Soveris gemeinsam die Zwei-von-drei-Schwelle, und Soveris signiert nur innerhalb des Rahmens mit, den du im Voraus gesetzt hast – etwa Auszahlungen an Ziele, die du vorab freigegeben hast. Soveris hält nie zwei Anteile, signiert nie allein und entscheidet nie über eine Auszahlung.

6 Die Bedrohungen, und was bleibt

Der ehrliche Weg, Sicherheit darzustellen, ist nicht zu behaupten, es gebe keine Bedrohungen, sondern die echten durchzugehen und für jede zu zeigen, was die Architektur dagegen tut – einschließlich dort, wo ein Restrisiko bleibt. Was folgt, ist das vollständige Bild; das Fundament aus Abschnitt 2 trägt die strukturellen Zeilen, die Leitplanken aus Abschnitt 4 die konfigurierbaren.

Bedrohung	Wie Fundament und Leitplanken darauf antworten	Was bleibt
Interessenkonflikt – dein Vermögen finanziert ein Geschäft	Kein Handelstisch, kein Verleihbuch, kein Staking deiner Coins. Durch die Architektur hält Soveris einen Anteil von dreien und kann dein Vermögen gar nicht bewegen – es gibt nichts zu rehypothekieren.	Nichts. Diese Fehlerart ist strukturell beseitigt, nicht weggeredet.
Der Verwahrer wird insolvent oder verschwindet	Soveris, das einen Anteil hält, kann dein Vermögen nicht stranden lassen. Deine zwei Anteile PRIMARY und BACKUP steigen ohne uns aus, und eine Insolvenz löst ein einmaliges, offline laufendes Werkzeug zum Selbstausstieg aus (Abschnitt 7).	Du musst deine Wiederherstellungs-Passphrase auffindbar halten; die verschlüsselte Sicherung ist ohne sie nutzlos.
Auszahlungen werden eingefroren oder angehalten	Es gibt keinen Auszahlungsknopf, den wir abschalten könnten. Du hältst zwei der drei Anteile und versendest jede Transaktion selbst; Soveris kann dein Vermögen nicht einsperren.	Ein entschlossener staatlicher Akteur kann dich weiterhin direkt verfolgen – doch der Hebel sitzt nicht bei Soveris.
Dein Telefon geht verloren oder wird gestohlen	Das tägliche Signieren ist durch Biometrie am Sicherheitselement gesichert, nicht durch einen Code – ein Dieb, der dir beim Tippen einer PIN zugesehen hat, kann also dennoch nicht signieren. Größere Bestände liegen hinter der zeitgesperrten Wiederherstellung, die der Dieb nicht erreicht.	Was innerhalb deiner Alltagslimits liegt, bleibt erreichbar, bis du das Gerät widerrufst; danach macht eine Erneuerung der Anteile es ungültig.
Ein unumkehrbarer Eigenfehler – falsche Adresse, Vertipper	Das Pro-Transaktions- und das Tageslimit, die Auszahlungs-Sperrfrist und die Aktivierungssperre der Empfänger-Whitelist schaffen jeweils einen Moment, einen Fehler abzufangen, bevor er das Haus verlässt.	Eine Sendung innerhalb deiner eigenen Limits, an eine von dir freigegebene Adresse, geht dennoch durch; die Leitplanken begrenzen Fehler, sie schaffen sie nicht ab.
Zwang oder ein „Schraubenschlüssel-Angriff"	Die Wiederherstellung aus dem BACKUP ist zeitgesperrt, eine erzwungene Wiederherstellung ist also nie sofort: sie meldet sich auf jedem Kanal und bleibt das ganze Fenster über abbrechbar, und die Asymmetrie verhindert, dass ein Angreifer die Sperre herunterdreht. Der Nachlass liegt hinter der Sperre.	Ein alltäglicher Betrag innerhalb der Limits ist unter unmittelbarem Druck dennoch erreichbar, und der Abbruch hängt daran, dass eine Warnung jemanden erreicht, der handeln kann. Die Sperre schützt den Nachlass, nicht die Alltags-Wallet – so gewollt.
Eine gekaperte Sitzung fügt ihre eigene Auszahlungsadresse hinzu	Die Aktivierungssperre der Empfänger-Whitelist macht eine neu hinzugefügte Adresse erst nutzbar, wenn deine Sperrfrist abgelaufen ist – bis dahin bist du benachrichtigt und kannst abbrechen.	Eine erstmalige, sauber wirkende Adresse, die du dich täuschen lässt zu listen und auszusitzen, kann von dir dennoch freigegeben werden – gemindert, nicht beseitigt.

Bedrohung	Wie Fundament und Leitplanken darauf antworten	Was bleibt
SIM-Swap oder Konto-Übernahme	Dein Konto-Passwort ist der kryptografische Anker, kein SMS-Code; die empfohlene Konfiguration nutzt eine zeitbasierte Code-App (Authenticator, TOTP) plus Biometrie. Eine vollständige Übernahme erlaubt einem Angreifer nur, eine Wiederherstellung zu *beantragen* – was die Zeitsperre auslöst und dich überall benachrichtigt.	Eine Konfiguration, die auf SMS-gestützte Anmeldung setzt, ist eben deshalb an eine niedrigere Guthabengrenze gebunden.
Ein Innentäter bei Soveris	Ein Anteil kann nicht signieren. Kein Mitarbeiter, auf keiner Zugriffsebene, kann allein eine Signatur erzeugen; die Mandantentrennung und die Mehrfachfreigabe fügen weitere Riegel hinzu.	Ein Angreifer müsste zusätzlich und unabhängig einen zweiten Anteil kompromittieren, den nur du hältst.
Ein Einbruch in Soveris-Systeme	Es gibt nirgends einen vollständigen Schlüssel zu stehlen. Ein Einbruch liefert einen einzelnen Anteil – für sich genommen nutzlos. Die Mandantentrennung und die Erneuerung alle neunzig Tage begrenzen den Schaden.	Ein Angreifer bräuchte weiterhin einen zweiten, unabhängig gesicherten Anteil.
Ein gegen Soveris gerichteter Gerichtsbeschluss	Ein Beschluss, der den Anteil von Soveris erzwingt, erzwingt einen Anteil, der allein nicht signieren oder Vermögen bewegen kann. Soveris ist nicht in der Lage, das Vermögen herauszugeben.	Ein entschlossener staatlicher Akteur kann dich weiterhin direkt verfolgen; bei Soveris sitzt der Hebel nicht.
Ein über Jahre still kompromittierter Anteil	Die automatische Erneuerung alle neunzig Tage, dazu die ereignisgesteuerte Erneuerung, macht alte Anteile ungültig und erhält deine Adresse.	Sie verengt das Fenster auf einen Erneuerungszyklus, statt es zu beseitigen: ein Anteil, der erbeutet *und* innerhalb eines Fensters mit einem zweiten gepaart wird, könnte dennoch etwas bedeuten.
Ein verlorener Faktor oder ein totes Gerät	Du hantierst nie mit einem rohen Seed. Ein verlorenes Telefon ist in unter einer Minute wiederhergestellt; ein verlorener Faktor wird aus dem BACKUP neu abgeleitet.	Den Verlust eines Faktors überlebst du nur, solange der andere auffindbar bleibt – wozu eben die regelmäßige Gegenprobe (Abschnitt 3) da ist. Der vollständige Verlust jedes Wegs ist in Abschnitt 9 behandelt.
Ein betrügerischer Erbanspruch	Erben sind vorab eingetragen, beim Erbfall über die Identität abgeglichen, gegen mehrere amtliche Dokumente geprüft und durch eine Wartefrist von vierzehn Tagen gehalten, bevor sich etwas ändert.	Übliche Wege des Nachlassbetrugs sind durch die Mehr-Dokumente-Prüfung und die Vorab-Eintragung begrenzt, nicht beseitigt.

Bedrohung	Wie Fundament und Leitplanken darauf antworten	Was bleibt
Ein kompromittiertes Telefon-Betriebssystem	Ein Geräte-Implantat auf dem Niveau eines staatlichen Akteurs liegt außerhalb des normalen Kunden-Bedrohungsmodells; ihm begegnen teils das Ownership BACKUP und die Wiederherstellungs-Sperrfrist.	Ein vollständig kompromittiertes Gerät während alltäglicher Ausgaben innerhalb der Limits ist exponiert. Das sagen wir offen.
Eine vergiftete oder ausgetauschte Zieladresse	Das Screening warnt, bevor du an eine markierte Adresse sendest – du entscheidest stets, ob du fortfährst; die Empfänger-Whitelist mit ihrer Aktivierungssperre stumpft Adress-Tausch-Angriffe ab.	Eine erstmalige, sauber wirkende Angreifer-Adresse kann von dir dennoch freigegeben werden – gemindert, nicht beseitigt.

Für die zwei Kontrollen, die am leichtesten zu verwechseln sind – die Wiederherstellungs-Sperrfrist und die Aktivierungssperre der Whitelist – und für die dritte zeitbasierte Schutzmaßnahme, die Auszahlungs-Sperrfrist, siehe Abschnitt 4: drei verschiedene zeitbasierte Schutzmechanismen, die drei verschiedene Aufgaben erfüllen.

7 Unabhängigkeit als Bauprinzip

Die tiefste Furcht in der Verwahrung ist die Furcht vor der Gegenpartei: *Was, wenn die Einrichtung, auf die ich baue, sich gegen mich wendet oder schlicht verschwindet?* Soveris antwortet darauf nicht mit einer Beruhigung, sondern mit einer Eigenschaft des Systems.

Du kannst jederzeit gehen

Soveris zu verlassen ist kein Entgegenkommen, das wir gewähren; es ist eine eingebaute kryptografische Fähigkeit. Deine zwei Anteile – PRIMARY auf deinem Telefon und dein BACKUP – genügen für sich, um eine Transaktion zu signieren und dein Vermögen in jede Wallet deiner Wahl zu bewegen. Keine Mitwirkung von Soveris ist nötig, und keine kann verweigert werden. Im kryptografischen Anker sitzt nirgends eine Anbieter-Abhängigkeit; jede externe Komponente, die das System nutzt, ist austauschbar.

Wenn Soveris morgen verschwände

Würde Soveris zahlungsunfähig, dein Vermögen wäre es nicht. Soveris speichert voreingestellt die einzige verschlüsselte Kopie deiner Sicherung, freigegeben nur unter strenger Prüfung und der Wiederherstellungs-Sperrfrist – eine Haltung gegen Diebstahl, keine Abhängigkeit. Damit die Ausstiegsgarantie selbst in diesem Fall hält, unterhält Soveris einen Notfallplan: scheitert das Unternehmen, erhält jeder Kunde seine eigene verschlüsselte Sicherung zusammen mit einem einmaligen, vollständig offline laufenden, quelloffenen Werkzeug zum Selbstausstieg, ausgeliefert sowohl in der App als auch über ein öffentlich gespiegeltes Repository.

Das Werkzeug hält keine Schlüssel. Du führst es offline aus, entschlüsselst deine Sicherung mit deiner eigenen Wiederherstellungs-Passphrase und nutzt deine Anteile PRIMARY und BACKUP, um einen Ausstieg zu signieren und ihn über jeden Weg zu senden, den du magst. Die freigegebene Sicherung ist

ohne deine Passphrase nutzlos, dir sie zu senden fügt also kein Risiko hinzu. In diesem Fall steuert Soveris keinen Anteil bei, signiert nichts und bewegt nichts. Du bist der einzige Handelnde – genau wie an jedem anderen Tag.

Das ist die praktische Bedeutung von Selbst-Souveränität: der Teil des Systems, den du nicht persönlich einsehen kannst – unsere Server, unser HSM –, ist zugleich der Teil, den du nicht brauchst, um dein eigenes Vermögen zurückzuholen.

8 Wie Soveris rechtlich steht

Weil die Wallet von einem Schwellenschema zwei von drei bestimmt wird, in dem Soveris nur einen einzelnen Mitsignier-Anteil hält – nie einen vollständigen Schlüssel und nie ein Quorum –, kann Soveris dein Vermögen nicht aus eigener Kraft bewegen oder einen Schlüssel rekonstruieren, und du allein initiierst und versendest jede Transaktion. Unsere abgewogene Einschätzung dieser Architektur ist, dass Soveris als nicht-verwahrender Software- und MPC-Infrastrukturanbieter handelt und nicht als Krypto-Verwahrer – und nach dieser Einschätzung die regulierte Tätigkeit der Krypto-Verwahrung im Sinne der MiCA (Verordnung (EU) 2023/1114, Artikel 3(1)) nicht ausüben würde; in Deutschland beaufsichtigt nach dem Kryptomärkteaufsichtsgesetz (KMAG). Wir formulieren dies als eine auf der oben beschriebenen Struktur beruhende Einschätzung, die wir vor dem Marktstart mit qualifiziertem Rechtsbeistand bestätigen.

Dieses Papier dient allein der Information. Es ist keine Rechts-, Steuer-, Finanz- oder Anlageberatung und kein Angebot eines Produkts oder Dienstes; die rechtliche Einordnung von Soveris ist eine abgewogene Einschätzung der hier beschriebenen Architektur, die wir vor dem Marktstart mit qualifiziertem Rechtsbeistand bestätigen.

9 Ehrliche Grenzen

Ein Dokument, das seine eigenen Grenzen benennt, ist eines, dem du bei den Aussagen vertrauen kannst, die es trifft. Hier, offen, ist, wovor Soveris dich nicht schützen kann.

Verlierst du beide deiner Geheimnisse, kann niemand dein Vermögen zurückholen. Der einzige unrettbare Zustand im ganzen System ist der gleichzeitige Verlust *beider* – des Konto-Passworts und der Wiederherstellungs-Passphrase. Den Verlust eines überlebst du immer – das verbleibende Geheimnis stellt das verlorene wieder her. Der Verlust beider lässt keinen Weg, für niemanden, auch nicht für Soveris. Das ist der notwendige Preis echter Souveränität: dieselbe Eigenschaft, die uns außerstande setzt, dich zu verraten, setzt uns auch außerstande, einen Totalverlust zu überschreiben. Wir machen dieses Ergebnis so unwahrscheinlich, wie Sorgfalt und guter Entwurf es zulassen – die mehreren Sicherungswege und die verpflichtende regelmäßige Gegenprobe aus Abschnitt 3 sind eben dazu gebaut, einen einzelnen Verlust zu fangen, bevor er zu einem doppelten wird –, aber wir tun nicht so, als wäre es unmöglich.

Ein vollständig kompromittiertes Gerät ist während alltäglicher Ausgaben exponiert. Ein Implantat auf dem Niveau eines staatlichen Akteurs auf deinem Telefon liegt außerhalb des normalen Bedrohungsmodells, und ihm begegnen teils das Ownership BACKUP und die Wiederherstellungs-

Sperrfrist. Doch solange dein Gerät einem Angreifer vollständig gehört, sind Beträge innerhalb deiner Alltagslimits erreichbar. Der Nachlass hinter der Zeitsperre ist es nicht – die Alltags-Wallet schon.

Ein erzwungener Alltagsbetrag bleibt möglich. Die Wiederherstellungs-Sperrfrist ist gebaut, um den Großteil deines Vermögens vor Zwang zu schützen, und das tut sie. Doch sie schützt bewusst den *Nachlass*, nicht die Alltags-Wallet. Ein Angreifer, der unmittelbaren, körperlichen Druck ausübt, kann einen alltäglichen Betrag innerhalb der Limits dennoch erreichen. Wir sagen dir lieber genau, wo der Schutz beginnt und endet, als eine Garantie anzudeuten, die wir nicht halten können.

Zwei dieser drei Grenzen werden kleiner, je nachdem, wie du das System einstellst: halte deine Alltags-Wallet bescheiden, lege größere Bestände hinter den zeitgesperrten Nachlass – und der Großteil deines Vermögens bleibt jenseits eines kompromittierten Geräts wie einer erzwungenen Reichweite.

Uns ist auch bewusst, dass nach einem Vorfall mancher sagen wird „Soveris hielt die Schlüssel", wo Soveris einen Anteil von dreien hielt und nichts allein hätte signieren können. Wir benennen die Architektur lieber genau, hier und im Voraus, als eine bequeme Abkürzung für die Wahrheit stehen zu lassen.

Wir können dich nicht verraten, weil wir nicht allein handeln können. Alles Weitere in diesem Papier ist die Ausarbeitung dieses einen Satzes.