SeedProtector

Krypto-Schlüsselsicherung und Verwahrung mit SeedPro
UPSE-Verfahren (unique positional seed encoding)

KRYPTOVERWAHRUNG

OHNE LIZENZ

UPSE-SPLIT CODE VERFAHREN - GETEILTE AUFBEWAHRUNG
ZEITVERZÖGERTE RECOVERY - ONBOARDING - BEGLAUBIGUNG
RISIKO-STRESSTESTS - SMART KEY-SPEICHERUNG

WHITEPAPER
Stand 06/2025

TRUST4MONEY

WHITEPAPER SEEDPRO

UPSE-SPLIT CODE VERFAHREN

GETEILTE AUFBEWAHRUNG

ZEITVERZÖGERTE RECOVERY

ONBOARDING

BEGLAUBIGUNG

RISIKO-STRESSTESTS

SMART KEY-SPEICHERUNG

COMPLIENCE

EINLEITUNG ZU SEEDPRO

Im Kontext der sicheren Verwahrung kryptographischer Zugangsdaten, insbesondere BIP39-kompatibler Seedphrasen, stellt Seedprotector mit SeedPro ein neuartiges Verfahren vor, das eine **modulare, rechtskonforme und aufteilbare Speicherstruktur** ermöglicht. Ziel ist es mit Seedpro Seedphrasen **nicht als Klartextwörter** zu speichern, sondern in strukturierter Form, damit keine einzelne Komponenten als kryptografische Schlüssel im Sinne der europäischen Kredit-wesengesetze gelten. Dadurch ermöglicht SeedPro eine externe Verwahrung, z.B. bei **Banken, Notaren, Family Offices, Treuhändern oder Tresorverwahrern ohne Erlaubnispflicht** gemäß BaFin nach KWG §1 Abs.1a Nr.6 in Deutschland sowie FINMA und FMA in der Schweiz und Österreich.

DIE KRYPTO-SCHLÜSSELVER-WAHRUNG SEEDPRO

UNIQUE POSITIONAL SEED ENCODING (UPSE) - VERFAHREN

Die T4M GmbH - trust4money bietet mit ihrem Unternehmen **SeedProtector** und dem Kryptoverwahrungsprodukt **"SeedPro"** eine neuartige, modulare Lösung zur Aufbewahrung und Speicherung von BIP39-Seedphrasen an. Sie ist erstmals für Dienstleistungsunternehmen ohne Aufbewahrungslizenz integrierbar. Das dazu entwickelte Verfahren **(UNIQUE POSITIONAL SEED ENCODING - UPSE)** ermöglicht Endkunden, Banken, Treuhändern, Tresorverwahrern und FamilyOffices eine sichere Aufbewahrung und Speicherung von BIP39-Seedphrasen auf physischen, digitalen und biometrischen Medien. Es bietet eine hohe Flexibilität und **vollständige Rechtssicherheit gegenüber Behörden** in Deutschland (BaFin), Österreich (FMA) und Schweiz (FINMA).

SeedPro besteht im Jahr 2025 als einzige Krypto-Schlüsselverwahrungs-Lösung für externe Dienstleister die kompletten **Complience- Anforderungen** sowie einen umfangreichen **Risikostresstest** für potenzielle Gefahren beim Besitz und der Verwahrung von Kryptovermögensschlüsseln.

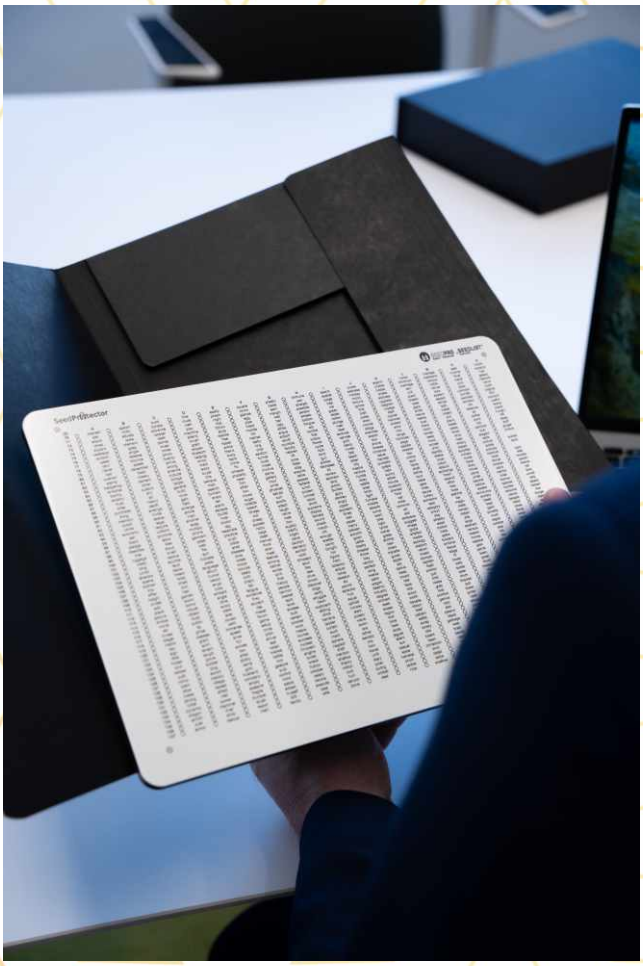
Die Architektur besteht aus einer **SeedList** (BIP39-Wortliste) **und einer KeycodeList** aus Metall sowie einem optionalen **NFC-Chip** mit PIN -und Code Speicherung. Die Schlüsselaufbewahrung SeedPro bietet für Endkunden, Unternehmen und Institutionen ein smartes Schutzkonzept für ihr eigenes digitales Vermögen und das ihrer Kunden. **Im Sinne der europäischen Kreditwesengesetze ist SeedPro vollständig rechtssicher.** Einzelne Komponenten gelten darin nicht als kryptografische Schlüssel, weswegen für die externe Aufbewahrung gemäß BaFin nach KWG §1 Abs.1a Nr.6 in Deutschland sowie FINMA und FMA in der Schweiz und Österreich keine Lizenzpflicht gefordert ist. Dadurch ermöglicht Seedpro eine externe Verwahrung z.B. durch **Notare, Banken, Treuhänder, Family Offices, und Tresorverwahrer**, die nicht über eine Erlaubnis zur Aufbewahrung verfügen. Seedpro besitzt **mehrschichtige Zugriffskontrollen**, sowie **zeitverzögerte Zugriffe** und **Multi-Personen-Integrationen.** Neben einer standardisierten rein physischen Seedphrasen-Speicherung können mit SeedPro zusätzlich digitale und biometrische Speichermedien wie NFC -Cards und -Coins in den Schutz eingebunden werden. So können sicherheitsbeteiligte Personen und Institutionen integriert werden, um die Flexibilität und die Absicherung zu erhöhen.

SEEDPRO „UPSE VERFAHREN“

SeedPro wendet ein Verfahren an, mit dem eine BIP39-**Seedphrase in Positionscodes** übersetzt wird. Diese sogenannten SeedCodes von Wallets repräsentieren die Positionen der Seedwörter innerhalb der standardisierten BIP39-SeedList (2048 Wörter aus Bitcoin Improvement Proposal-39). Sie wird für jeden Anwender individuell in einer zufälligen Reihenfolge neu hergestellt, wodurch der SeedCode selbst bei gleichen Wörtern immer einzigartig ist. Die BIP39-SeedList entspricht dem Format DINA4 und wird auf Aluminium-Verbundplatten vorder- und rückseitig im sicheren Thermoverfahren bedruckt. Sie sind dadurch **wasserfest, kratzfest UV-strahlungssicher und schwer entflammbar.** Aufgrund ihrer Größe ist sie **tresor- und aktenfähig** und im Gegensatz zu deutlich kleineren Sicherungen gut aufzubewahren und nicht so leicht zu verlieren.

STRUKTURIERUNG DER BIP39 SEED-WORTLISTE

Die BIP39-SeedList wird in eine Matrix mit **15 Spalten (A–O)** und **137 Zeilen (1–137)** überführt. Jeder Eintrag in der Liste lässt sich somit durch einen alphanumerischen Code wie z.B. **"F73"** eindeutig referenzieren.



UMWANDLUNG DER SEEDPHRASE

Eine standardisierte 12- oder 24-Wort-Seedphrase wird in 12 bzw. 24 dieser Positionscodes umgewandelt: **mystery garden rival ... → H79 F61 K44 ...**

SPEICHERUNG DES SEEDCODES

Der resultierende SeedCode, z.B. "H79 F61 K44 ..." ist ohne Kontext oder Zusatzinformation der BIP39- SeedList wertlos. Zur Wiederherstellung der Seedphrase ist diese separate SeedList notwendig. Der SeedCode kann auf Datenträgern wie Festplatten, NFC-Cards, Coins oder Chips dauerhaft gespeichert und nur mit der BIP39 SeedList in Seedwörter und Phrase umgewandelt werden.

KOMPONENTENMODELL

SeedProtector teilt die Informationen in 5 voneinander getrennten Komponenten auf und integriert sie in das codierte und aufgeteilte Kryptoschlüssel-Sicherheits- und Verwahrungskonzept SeedPro:

1 HARDWAREWALLETS

Hardwarewallets sind spezialisierte Geräte zur sicheren Speicherung von Seedphrasen. Sie ermöglichen die **Generierung und Speicherung privater Schlüssel**, die **Ableitung von Walletadressen** sowie die **Validierung und Signatur von Transaktionen** – ohne dass die Schlüssel das Gerät verlassen. Im SeedPro-Modell erzeugen die Geräte die Quelle der Wortauswahl und bilden die Seedphrase für den PrivateKey. In Kombination mit einem SeedCode und der zugehörigen SeedList können die Seedwörter zurück gebildet werden, die im Notfall für eine mögliche Wiederherstellung von Wallets benötigt werden.

2 SEEDPHRASEN

Seedphrasen sind nach der Bildung des SeedCode zur Vernichtung vorgesehen. Im Zielsystem von SeedPro wird die klassische Seedphrase auf Papier oder anderen physischen Medien vernichtet, sobald aus der Kombination von BIP39-SeedList und der individuellen Wortauswahl der SeedCode gebildet, explizit geprüft und sicher gespeichert wurde.

Dadurch wird **das Sicherheitsrisiko der Seedphrase im Klartext** minimiert, das beim unerlaubten Auffinden oder bei einer Herausgabe und einem Missbrauch entsteht.

3 AKTIVIERUNGS-PIN

Sie dienen zur Authentifizierung oder als kryptografischer Zusatzfaktor, mit der die Walletsoftware aktiviert wird.

4 SEEDLIST

Die SeedList ist als **Kernstück der Sicherung** zu verstehen. Sie basiert auf der vollständigen BIP39-Wortliste mit allen 2048 Seedwörtern. Jede Wortliste wird in eine individuell neu angeordneter Positionsreihenfolge gebracht. Diese SeedList ist die Quelle, der vom Wallet ausgewählten 12 oder 24 Seedwörter. **Mit der SeedList und dem SeedCode kann die ursprüngliche Seedphrase rekonstruiert werden.**

5 SEEDCODE

Der strukturierte Positionscode kann z.B. auf Papier, oder Metallplatte alphanummerisch oder als QR-Code sowie digital auf USB-Sticks, Festplatten, NFC-Chips, NFC-Cards oder Coins gespeichert werden. Alle Komponenten können unabhängig voneinander von externen Dienstleistern gespeichert, verteilt und verwahrt werden. Kein einzelnes Element bildet für sich einen vollständigen privaten Schlüssel (PrivateKey).

VERTEILUNG UND AUFBEWAHRUNG DER KOMPONENTEN

Das Hardwarewallet befindet sich beim Kryptobesitzer selbst, bei der Bank oder beim Tresorverwahrer. Es darf mit dem SeedCode oder SeedList aber niemals in Kombination mit der AktivierungsPIN aufbewahrt werden. Der **SeedCode** befindet sich z.B. auf NFC-Card, Chip oder Metall-SeedCodeList beim Kryptobesitzer selbst oder bei der Bank, beim Tresorverwahrer oder bei Sicherheitsbeteiligten wie Kindern, Ehepartnern, Geschäftspartnern, Treuhändern oder Notaren. Der Code darf mit Wallet oder PIN aber niemals in Kombination mit der SeedList aufbewahrt werden. Die **SeedList (BIP39-Wortliste)**: Sollte nur geschützt in Tresoren oder bei besonders vertrauenswürdigen Stellen wie Tresorverwahrern, Treuhändern oder Notaren hinterlegt werden. Sie kann zusammen mit Wallets oder PIN, allerdings niemals in Kombination mit dem SeedCode aufbewahrt werden. Die **Wallet-Aktivierungs-PIN** befindet sich beim Kryptobesitzer selbst und ist als zusätzlicher Schutzfaktor vorzugsweise bei Treuhändern, Notaren oder Tresorverwahrern zu lagern. Sie darf mit Seedlist oder SeedCode aber niemals in Kombination mit dem Wallet aufbewahrt werden.

REGULATORISCHE BEWERTUNG

Da der SeedCode keine Seedwörter im Klartext oder kryptografische Schlüssel darstellt, sondern lediglich strukturierte Positionsangaben enthält, handelt es sich nicht um die Verwahrung eines privaten Schlüssels gemäß der europäischer Kreditwesengesetze (z.B. KWG § 1 Abs. 1a Nr. 6.) Die Verwahrung einzelner Komponenten kann somit **rechtskonform ohne Erlaubnis der jeweiligen Finanzbehörden,** wie BaFin in Deutschland sowie FINMA und FMA in der Schweiz und Österreich erfolgen, solange keine Stelle Zugriff auf alle relevanten Komponenten gleichzeitig besitzt.

BACKUP BIP-39 SEEDLIST

Wiederherstellungen von registrierten BIP-39-SeedLists sind eine diskrete, wählbare BackUp Option, wenn Verwahrungen von SeedLists scheitern. Die Speicherung erfolgt unpersonalisiert mit einem geheimen Recovery-Word + Position der BIP-39 SeedList, das wahlweise beim Sicherungsanbieter, Treuhänder, Bank, Notar oder Family-Office hinterlegt werden kann.

VORTEILE UPSE VERFAHREN

Die Vorteile des UPSE-Aufbewahrungsverfahrens, wie SeedPro liegen darin, dass es modular und verteilbar ist, wodurch es die wenigsten Risiken aufweist. Der SeedCode, die SeedList sowie PIN und Wallet können wahlweise getrennt gespeichert werden und Dienstleistungsunternehmen sind erstmals rechtskonform integrierbar. Das Verfahren erfordern keine Lizenzpflicht für externe Verwahrstellen. Das UPSE-Aufbewahrungssystem ist standardkompatibel mit vollständigen, öffentlichen BIP39-Wortlisten und ermöglicht eine Rekonstruktion. Es bietet durch die Codierung der Seedwörter und die Aufteilbarkeit der Komponenten auf Dienstleister die bisher höchste Flexibilität und Sicherheit für Endkunden, Unternehmen, Notare, Treuhänder, FamilyOffices und Behörden gegenüber anderen Verwahrungssystemen und Risiken. Die Seedphrase ist allein nicht rekonstruierbar ohne eine SeedList und einen SeedCode.

ANWENDUNGSBEISPIELE

Als sicher verwahrt gilt z.B. ein SeedCode und PIN in einem Tresor- oder Bankschließfach, sowie die SeedList bei Treuhänder und das Wallet beim Kryptobesitzer. Der PIN-Aktivierungscode sollte separat im Safe aufbewahrt werden. Das UPSE-Aufbewahrungssystem SeedPro bietet eine strukturierte, sichere und regulatorisch zugelassene Alternative zur klassischen Seedphrasen-Verwahrung.

KRYPTO-SICHERUNG UND VERWAHRUNG

MIT SEEDPRO IM UPSE-VERFAHREN

CODIERUNG SEEDWORDS

die Codierung der Seedwörter wird als Übertragung der Wallet-Seedphrase in einen SeedKey, bestehend aus Positionsnummern der gesamten BIP39-Seedlist verstanden, um eine höhere Flexibilität und Sicherheit des PrivateKeys zu gewährleisten. Dazu wird der SeedKey mit eine Metall-Seedlist mit individuell angeordneten Seedwörtern auf eine Keylist aus Papier oder Metall übertragen.

SPEICHERUNG SEEDKEYS

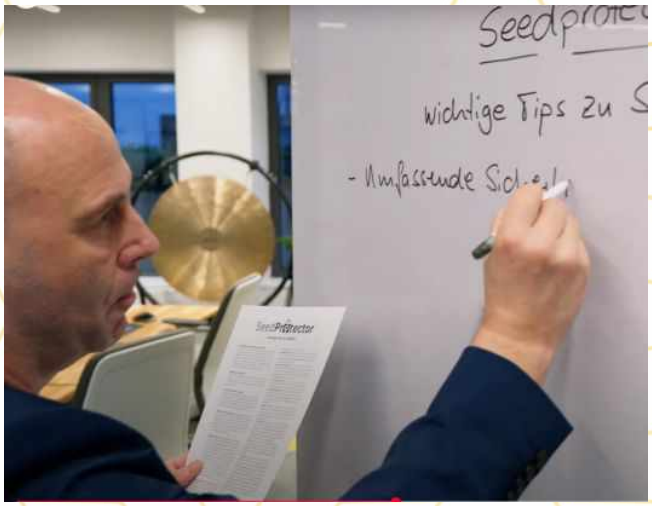
als Speicherung wird das Abspeichern des SeedKeys auf verschiedenen Medien verstanden, um eine Teilbarkeit der Seedlist mit anderen Personen und Institutionen und eine Kopierbarkeit des SeedKeys herstellen zu können. Als digitale und biometrische Speichermedien kommen NFC-Chips in verschiedenen Ausführungen zum Einsatz, um eine einfache Auslesbarkeit mit Mobiltelefonen zu gewährleisten sowie Festplatten und USB-Speicher. Physisch werden SeedKeys auf Metallplatten verwahrt.

VERWAHRUNG BIP-39 SEEDLISTS

als Verwahrung wird die externe Aufbewahrung von SeedLists bei Verwahrern wie Banken, Treuhänder, Tresoranbieter und FamilyOfiffes sowie in bestimmten Fällen die Verwahrung von SeedKeys angesehen.

RISIKOANALYSE SEEDPRO

Die Risikoanalyse beschreibt potenzielle Gefahren beim Besitz und der Verwahrung von Kryptovermögens-schlüsseln – konkret im Vergleich zum SeedPro-UPSE Verfahren. Es werden klassische Risiken und deren Auswirkungen erläutert sowie die spezifischen Schutz-mechanismen von SeedPro dargestellt.



1 Verlust / Vergessen

Ursache: SeedCode oder KeyCode wird verlegt; PIN wird vergessen

Auswirkung: Zugriff auf das Kryptovermögen dauerhaft verloren

SeedPro-Schutz: Trennung der Komponenten erlaubt gezielte, redundante Sicherung. Der KeyCode kann separat (z.B. bei Notar, Bank, Family Office) aufbewahrt werden. Die PIN ist optional und kann dokumentiert oder durch Dritte verwahrt werden

2 Physische Zerstörung

Ursache: Brand, Wasser, Umwelt, Defekte bei Speicher-trägern

Auswirkung: Teilweiser oder vollständiger Verlust einer Komponente

SeedPro-Schutz: SeedCode kann auf robustem Medium (z.B. Metallplatte) gespeichert werden. Geografisch getrennte Kopien möglich (z.B. bei Family Office und privat) Wiederherstellungsoption buchbar.

3 Missbrauch durch Dritte

Ursache: Unbefugter Zugriff auf SeedCode, KeyCode und PIN gleichzeitig

Auswirkung: Kompletter Diebstahl des Kryptovermögens

SeedPro-Schutz: Kein einzelner Teil erlaubt Zugriff. Multi-Faktor-Zugang verhindert unmittelbaren Zugriff. Kompo-nenten können unter verschiedenen physischen und rechtlichen Akteuren verwahrt werden.

4 Technologischer Fehler

Ursache: Falscher SeedCode, veraltete Wortlisten, inkom-patible Wallets

Auswirkung: Wiederherstellung des Wallets schlägt fehl

SeedPro-Schutz: Verwendung der standardisierten BIP39-Wortliste. Automatisierte Tools zur Code Ein-/und Auslesung und Validierung möglich. Kompatibel mit Wallets (z.B. Ledger, Bitbox, Trizor)

5 Tod / Erbschaft / Blackout

Ursache: SeedCode oder PIN bekannt, aber KeyCode nicht auffindbar (z.B. bei plötzlichem Todesfall)

Auswirkung: Zugriff für Erben unmöglich

SeedPro-Schutz: Schlüsselkomponenten können gezielt verteilt werden (z.B. SeedCode an Erben, KeyCode beim Notar). Testamentarisch geregelter Zugriff möglich, ohne dass während der Lebenszeit jemand alleinigen Zugriff hat.

6 Rechtliche Risiken

Ursache: Verwahrung durch Dritte führt zu BaFin-relevantem Tatbestand

Auswirkung: Strafbarkeit, Lizenzverstoß, Unklarheiten im Rechtsraum

SeedPro-Schutz: SeedCode, KeyCode und PIN sind jeweils für sich kein kryptografischer Schlüssel im Sinne des KWG. Rechtlich sichere Verwahrung durch externe Parteien möglich, ohne BaFin-Lizenzpflicht.

7 Verwechslung /Fehl-bedienung

Ursache: Vertauschte Codes, falsche Eingabe (z.B. a137 statt A137)

Auswirkung: Wiederherstellung des falschen Wallets, Datenverlust

SeedPro-Schutz: Strukturiertes Codierungssystem (z.B. A–O und 1–137) senkt Fehlerrisiko. Zusatzfunktionen wie Rückwärtskompatibilität.

8 Offenlegung / Kopierbarkeit

Ursache: SeedCode wird fotografiert oder unverschlüsselt gespeichert, KeyCode ausgelesen.

Auswirkung: Unbemerktes Erstellen von Kopien durch Dritte

SeedPro-Schutz: SeedCode allein ist wertlos – Zugriff erfordert weitere Faktoren. KeyCode kann auf krypto-grafisch gesichertem Medium gespeichert werden (z.B. NFC mit Passwortschutz). Kein digitaler Klartext-Speicher erforderlich.

9 Ausfall von Drittparteien

Ursache: Verwahrstelle existiert nicht mehr (z.B. Insolvenz des Notars oder Treuhänders)

Auswirkung: Zugang dauerhaft blockiert

SeedPro-Schutz: SeedCode verbleibt beim Nutzer oder in dessen Erbmasse. Redundante Verwahrketten (z.B. mehrere NFC-Karten bei unterschiedlichen Stellen) möglich. Notfallwiederherstellung über Ersatzzugangs-verfahren möglich.

SeedPro begegnet den klassischen Risiken bei der Selbstverwahrung von Krypto-Schlüsseln mit einem mehrschichtigen, modularen Sicherheitskonzept. Durch die Trennung von SeedCode, KeyCode und optionaler PIN sowie die Kompatibilität mit rechtlichen Rahmen-bedingungen entsteht ein hoher Schutz gegen Verlust.

ONBOARDING-PROTOKOLL

Es werden im Onboardingprotokoll alle Schritte, Teilnehmer, Zeitpunkte, Seriennummern dokumentiert und Empfangsbestätigungen als Nachweis über die Aushändigung von SeedCode, KeyCode, PINRollen-klärung ausgehändigt. Darin wird z.B. dokumentiert, wer was verwahrt und welche Bedingungen für die Heraus-gabe gelten. Im Erklärungsvermerk wird z.B. festgehalten, dass bestätigt wird, das Wallet selbst eingerichtet zu haben.

NOTAR TATSACHENFESTSTELLUNG

Notare oder bevollmächtigte Zeugen (z.B. Rechtsanwälte, geschulte Mitarbeiter) können Tatsachenfeststellungen formell dokumentieren und bestätigen (z.B. den Ablauf, das Vorliegen von Hardwarewallet, die Verwahrung etc.). Parteien selbst können Tatsachen in gemeinsamen Protokollen feststellen. Allerdings steigt die formelle Wirksamkeit, wenn ein Notar oder unabhängiger Zeuge die Feststellung beurkundet oder bestätigt.

PRÜFPUNKTE FÜR DAS SEEDPRO-ON-BOARDING

Neben weiteren Prüfpunkten wird beim Onboarding bestätigt, dass der SeedPro-Onboardingprozess **in Gegenwart der genannten Personen** unter **Einhaltung aller dokumentierten Prüfpunkte und Verfahrensschritte** durchgeführt wird. Es wird z.B. festgestellt, dass

1. alle anwesenden Personen im Protokoll korrekt aufgeführt sind,
2. das Hardwarewallet ungeöffnet und original verpackt übergeben wurde,
3. das Wallet erstmalig in Gegenwart in Betrieb genommen wurde,
4. der Passkey (PIN) zur Anmeldung erstellt und dokumentiert wurde,
5. die 24 Wörter umfassende Seedphrase erstellt, geprüft und gesichert wurden,
6. die Umwandlung der Seedphrase in den KeyCode korrekt erfolgte und auf das SeedPro-System übertragen wurde
7. alle relevanten Sicherheits- und Vertraulichkeitsmaßnahmen eingehalten wurden,
8. die Seedphrasen nach der KeyCode-Übertragung vollständig und gemeinschaftlich vernichtet wurden,
9. die verantwortlichen Personen ihre jeweiligen Verpflichtungen zur sicheren Verwahrung der Seedliste, Keylist und Hardwarewallet übernommen haben,
10. alle Vertraulichkeits- und Sicherheitsvereinbarungen schriftlich festgehalten und von allen Parteien anerkannt wurden.

SPEICHERUNG DES SEED KEY-CODES AUF NFC

VERFAHRENSWEISE ZUR SPEICHERUNG DES SEED KEY-CODES AUF

SMART-NFC CHIP

Die Speicherungen von Key-Codes, die aus der BIP-39 Wortliste anhand der Wallet Seedphrase abgeleitet werden, können auf verschiedene Arten erfolgen. Eine sichere und praktische Anwendung ist die **Speicherung auf einem NFC Chip**, der in einer **Bitcoin-Münze** oder einer **Smart-Card** integriert ist. NFC steht für Near Field Communication, was auf Deutsch Nahfeldkommunikation bedeutet. Es ist eine Technologie, die es ermöglicht, drahtlos **Daten mit Geräten, wie Smartphones, Tablets auszutauschen,** wenn sie sich in unmittelbarer Nähe, wenige Zentimeter zueinander befinden. NFC kann zum Teilen von Dateien oder Informationen verwendet werden. Es ist eine einfache und preiswerte Technologie, die in allen modernen Geräten integriert ist. Sie erlaubt einen Datentransfer, der kein Internet, Bluetooth, Kabel oder Strom beim Chip benötigt.

VERFAHRENSWEISE ZUR SPEICHERUNG DES SEED KEY-CODES AUF

SMART-NFC BITCOIN-MÜNZE

Die goldene Smart-NFC-Bitcoin Münze ist von einer klaren PVC-Sicherungshülle umgeben, die das Auslesen der Informationen verhindert, solange sie nicht geöffnet wurde. Die Sicherungshülle ist mit einem Siegel versehen, das beim Öffnen getrennt werden muss. Damit ist sichergestellt, dass ein unerlaubtes Öffnen der Sicherungshülle und ein Auslesen des Chips mit den Informationen des KeyCodes bemerkt werden kann. Die Informationen werden einfach vom Smartphone mit einer beliebigen, kostenlosen NFC-Tag-Reader App z.B. NFC-Cool, oder NFC21 auf den NFC-Bitcoin Chip übertragen. Aus Sicherheitsgründen erfolgt das Auslesen im Flugmodus, in dem die Verbindung zum Internet unterbrochen ist. Nach der Benutzung des KeyCodes kann die Datei in der App wieder gelöscht und die Internetverbindung wieder hergestellt werden. Der Vorteil dieses Verfahrens ist, **dass der KeyCode keine Berührung mit dem Internet** hat und nur durch das **Öffnen der Schutzummantelung** des Coins möglich ist. Der Coin wird zur Aufbewahrung in einer Münzschatulle geliefert und kann mit anderen Wertgegenständen zusammen aufbewahrt oder in Tresoren eingelagert werden. Aufgrund der vergleichsweise günstigen Anschaffungspreise können **mehrere NFC-Coins mit den KeyCodes** beschrieben und unter **Personen oder Verwahrungsstellen aufgeteilt** werden. **Paritäten oder Majoritäten** können durch das Splitting des Codes in beliebige Teile hergestellt werden, um zum Beispiel 2/3 Mehrheiten bei der Rekonstruktion der Seedphrase anhand des KeyCode Fragments (z.B. jeweils 1 oder 2/3 Code pro NFC Card) festzulegen.

Zum Beispiel teilen sich 3 Personen einen KeyCode gleichberechtigt mit jeweils 8 oder 16 Teil-Informationen. Durch das beschriebene aufgeteilte, Splittingverfahren für **KeyCodes, die aus Seedphrasen** gebildet werden, kann als zusätzliche Sicherheit **eine Zeitverzögerung** integriert werden, um einen **Herausgabezwang z.B. durch Erpressung** entgegen zu wirken. Es kann eine zusätzliche Person oder Institution integriert werden, die erst mit einer zuvor vereinbarten Zeitverzögerung von z.B. 24 Stunden das fehlende Codefragment seines NFC-Bitcoinmünz-speichers oder der NFC-Speichercard offenbart.

Als Vertrauenspersonen können zum Schutz **Treuhänder, Notare, Banken oder Familienmitglieder** integriert werden. Beim Einsatz von Bitcoinmünzen zur Speicherung des KeyCodes, die aus Seedphrasen gebildet werden ist es empfohlen, **Ersatzcoins herzustellen** und noch weitere Speichermedien und -Orte einzusetzen.

VERFAHRENSWEISE ZUR SPEICHERUNG DES SEED KEY-CODES AUF

SMART-NFC CARD

Die Verfahrensweise zur **Speicherung des KeyCodes auf NFC-Cards** ist die Selbe, wie mit einer NFC-Bitcoin-Münze (siehe Beschreibung Verfahrensweise zur Speicherung auf NFC-Coin). Anstelle der PVC-Schutzummantelung kann eine spezielle Schutzhülle, z.B. WallTrust verwendet werden, um einen **Datendiebstahl zu verhindern**, solange sich die Karte in der Hülle befindet. Die Hülle wird zur Sicherheit versiegelt, damit ein unerlaubtes Öffnen der Sicherungshülle und Entnahme der NFC Card und das Auslesen des Chips mit den Informationen des KeyCodes bemerkt werden kann. Die NFC Card hat das Format üblicher Scheckkarten und kann unauffällig in einem Kartenwallet mitgeführt werden. Die einfach schwarze Karte ist **unbedruckt und anonym** und gibt **keinen Hinweis auf den Einsatzzweck** und **den Informationsinhalt.** Die **zeitverzögerte Herausgabe** des KeyCode Fragments sowie die **Teilbarkeit für Paritäten und Majoritäten** ist ebenso gegeben, wie bei der smarten NFC-Bitcoin-Münze. Auch beim Einsatz von NFC-Cards zur Speicherung der KeyCodes, die aus Seedphrasen gebildet werden, ist es empfohlen, **Ersatzkarten herzustellen** und noch weitere Speichermedien und -Orte einzusetzen.

VERFAHRENSWEISE ZUR SPEICHERUNG DES SEED KEY-CODES AUF

SMART-NFC BIOCHIP

Biochips gelten als futuristische Lösung zum Schutz von KeyCodes. Damit können KeyCodes biometrisch im Körper aufbewahrt werden. Das Verfahren ist perfekt für alle, die sich höchste technische Sicherheit und Flexibilität wünschen. Eine Wiederherstellung der Seedphrase muss in bestimmten Fällen unverzüglich und anonym geschehen können. Der KeyCode kann unentdeckt als NFC-Implantat unter der Haut, z.B. and der Hand getragen werden und ist immer verfügbar. Der KeyCode wird damit unsichtbar und ist mit jedem NFC-Reader aus Smartphones per App genauso auslesbar, wie NFC-Smartcards und NFC-Smart-Bitcoinmünzen. Das Bio-Implantat kann durch jeden Arzt oder Piercer in wenigen Sekunden eingesetzt werden und ist allgemein verträglich. Der Eingriff ist schmerzarm und nach 1-2Wochen abgeheilt.

BACKUP BIP-39 SEEDLISTS

Die Registrierungsnummern der BIP-39 Seedlists können zur Sicherheit automatisch bis zu 3 Monate nach der Auslieferung anonym gespeichert werden, um für die Besitzer eine **Recovery-Option** während des Verschlüsselungs-Prozesses zu gewährleisten. Im Anschluss kann diese Speicherungsoption beim Hersteller oder einem Anbieter der Wahl fortlaufend beauftragt werden.

Die Wiederherstellung registrierter BIP-39-SeedLists erfolgt in einem geprüften anonymen Verfahren, wenn die eigene Verwahrung von SeedLists scheitert. Die Speicherung kann unpersonalisiert mit einem geheimen Recovery-Word + Position der BIP-39 SeedList wahlweise beim Sicherungshersteller, Treuhänder, Bank, Notar oder Family-Office erfolgen.

FAZIT ZUR SICHERUNG VON KRYPTO SCHLÜSSELN, DIE AUS SEDPHRASEN GENERIERT WERDEN

SEEDPRO MIT BIP-39 WORTLISTE

Seedpro kann durch die Umwandlung und Teilung von Seedphrasen, die aus dem PrivateKey von Wallets generiert werden als eine innovative Sicherung für Krypto-Schlüssel angesehen werden. Seedpro verbindet Complience-Fähigkeit gegenüber den heutigen Anforderungen, die Gesetze an die geteilte Aufbewahrung von Kryptoschlüssel stellen und ist im praktischen Einsatz einfach ohne Werkzeuge herzustellen.

Es liegt in der individuellen Entscheidung des Krypto-besitzers, ob mit SeedPro eine rein **physische Sicherung mit Metallplatten** ermöglicht, eine **digitale Aufbewahrung** mit NFC-Smart-Cards oder NFC-Smart Bitcoin-münzen oder eine **biometrische Speicherung** mit Smart-NFC-Biochips realisiert werden soll.

Die Aufteilungsmöglichkeiten von SeedPro Keycodes können vielfältig variiert und Personen und Institutionen in das Sicherheitskonzept integriert werden. Paritäten, Majoritäten und Zeitverzögerungen können individuell umgesetzt werden, um eine umfassende Sicherheit bei der Selbstverwahrung von Kryptologischen Schlüsseln zu erreichen.

Torsten Schmitz (Geschäftsführer)
T4M GmbH - trust4money **Seedprotector**
https://trust4money.de
https://seedprotector.de
Kaiserpassage 7, 72764 Reutlingen

Service Telefon.: 0800 - 333 7642
WhatsApp: 0170 - 22 82 295
Mail torsten@seedprotector.de
T4M GmbH - trust4money, HRB 761428 - UST. ID-Nr. DE300695324 - GF: Torsten Schmitz

PLATZ FÜR FRAGEN: