Bank Frick AG
Landstrasse 14
9496 Balzers
Liechtenstein

T +423 388 21 21
F +423 388 21 22
bank@bankfrick.li
www.bankfrick.li

Reg.-Nr.
FL-0001.548.501-4
MwSt.-Nr. 53884

Verwahrstrategie Bank Frick AG

Version 1.0 vom 1. Februar 2025

Diese Verwahrstrategie beschreibt die Grundsätze der sicheren, gesetzeskonformen Verwahrung von Kryptowerten und zugehörigen Private Keys gemäss den regulatorischen Anforderungen der Verordnung (EU) 2023/1114 über Märkte für Kryptowerte (MiCAR), der Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor (DORA) sowie des liechtensteinischen Aufsichtsrechts.

Überblick über die erbrachten Dienstleistungen

Bank Frick AG («Bank Frick») bietet im Rahmen ihrer Geschäftstätigkeit die Verwahrung von Kryptowerten einschliesslich der zugehörigen Private Keys an. Ziel ist es, die Kryptowerte ihrer Kund:innen sicher zu verwahren und ihren Kund:innen einfachen Zugang zu deren Token zu ermöglichen.

Regulatorische Anforderungen

Die Kund:innen nehmen zur Kenntnis, dass die Bank aufgrund internationaler, europäischer und/oder liechtensteinischer Rechtsvorschriften zur Bekämpfung von Geldwäscherei, organisierter Kriminalität und Terrorismusfinanzierung (u. a. Rechtsvorschriften betreffend Sorgfaltspflichten) verpflichtet ist, zu verwahrende Token von Kund:innen sowohl vor als auch während der Verwahrung insbesondere in Bezug auf deren Herkunft, Quelle und Authentizität bzw. auf allfällige Sperrvermerke hin zu prüfen und forensische Untersuchungen sowie andere Prüfungen durchzuführen, welche Bank Frick als relevant erachtet. Sämtliche Transaktionen unterliegen den geltenden Gesetzen zur Bekämpfung von Geldwäscherei.

Technische und prozessuale Aspekte der Verwahrung

Die Sicherheit der durch Bank Frick verwahrten Kryptowerte hat höchste Priorität. Bank Frick nutzt verschiedenste Technologien, um eine sichere Verwahrung von Kryptowerten sicherzustellen. Die Verwahrungslösung von Bank Frick ist nach CCSS Level III, SOC2 Type II und ISO 27001 zertifiziert.

Verwahrtechnologie

Multi-Party Computation (MPC): Technologie zur Generierung, Speicherung und Nutzung kryptografischer Signaturschlüssel zum Schutz von Kryptowerten und kryptografischen Instrumenten. Schlüssel, die in MPC erstellt und verwendet werden, befinden sich niemals an einem einzigen Ort. Vielmehr wird jeder Schlüssel so generiert, dass das Ergebnis zwischen zwei oder mehr Parteien geteilt wird, ohne dass eine bestimmte Partei mehr als ihren eigenen Anteil sieht, der für sich allein bedeutungslos ist. Darüber hinaus erfolgt die Signatur, ohne dass die Einzelteile jemals zusammengeführt werden. Das verhindert, dass Angreifer:innen auf eine Teilmenge von Rechnern gelangen und wichtiges Material extrahieren können. Da alle MPC-Teilnehmer:innen die Transaktion richtliniengemäss überprüfen müssen, ist es ausserdem nicht möglich, die Schutzmassnahmen zu umgehen, die zur Verhinderung des Missbrauchs eines Schlüssels installiert wurden.

Verwahrmodell

Bank Frick verwahrt ausschliesslich ausgewählte Kryptowerte und nutzt hierfür grundsätzlich das sogenannte Omnibus-Modell. Bei diesem Modell werden die Kryptowerte mehrerer Kund:innen auf gemeinsamen Distributed-Ledger-Adressen gespeichert und in Wallets gehalten, die von Bank Frick kontrolliert werden. Die individuelle Zuordnung der Kryptowerte zu den jeweiligen Kund:innen erfolgt operativ über ein internes Buchhaltungssystem und ist jederzeit nachvollziehbar. Aufgrund dieser eindeutigen Zuordnung gelten die Kryptowerte im Fall einer Insolvenz von Bank Frick als aussonderungsfähig.

Zugang zu Kryptowerten

Bank Frick bietet verschiedene (technische) Zugangswege zu ihrer Verwahrlösung an:

- Die Ein- und Auslieferung von Kryptowerten erfolgt über die Kundenberater:innen.
- Der Handel von Kryptowerten erfolgt über Kundenberater:innen, den Handelsdesk oder über das User Frontend (Online Banking). In ausgewählten Fällen ist auch der Handel über ein Application Programming Interface (API) möglich.

Die Verwahrlösung selbst ist zudem direkt an verschiedene Distributed Ledger (im Folgenden «Blockchains») angebunden. Die Einlieferung von Kryptowerten von Kunden in die Verwahrung von Bank Frick erfolgt grundsätzlich über die entsprechende Blockchain von Kundenadressen an die durch Bank Frick kontrollierten Adressen. Auslieferungen werden durch die Kundenberater:innen veranlasst und über die entsprechende Blockchain ausgeführt.

Wallet-Struktur

Bank Frick bietet folgende Wallet-Klassen an: Hot, Warm und Cold Wallets. Ziel dieser Wallet-Struktur ist es, höchste Sicherheit bei gleichzeitig hoher Verfügbarkeit der Kryptowerte zu ermöglichen.

- Hot Wallets: Hot Wallets sind ständig mit dem Internet verbunden und ermöglichen einen schnellen und einfachen Zugang zu den verwahrten Kryptowerten. Hot Wallets werden insbesondere für die Abwicklung von häufigen und kleinen Transaktionen verwendet.
- Warm Wallets: Für Verfügungen aus Warm Wallets ist eine manuelle Interaktion (Transaktionsfreigabe) von Mitarbeiter:innen von Bank Frick erforderlich. Warm Wallets werden für die Abwicklung von gelegentlichen und mittleren Transaktionen verwendet. Bank Frick hält einen grösseren Anteil der Kryptowerte von Kunden in Warm Wallets.
- Cold Wallets: Cold Wallets sind Wallets, die nicht mit dem Internet verbunden sind. Für Verfügungen aus Cold Wallets ist eine manuelle Interaktion (Transaktionsfreigabe) zwingend erforderlich, welche umfangreicher als die Transaktionsfreigabe im Fall von Warm-Wallet-Transaktionen ist. Cold Wallets werden für die Abwicklung von seltenen und sehr grossen Transaktionen verwendet. Bank Frick hält den grössten Anteil der Kryptowerte von Kunden in Cold Wallets.

Notfall- und Wiederherstellungspläne

Um die kontinuierliche Verfügbarkeit der Kryptowerte sicherzustellen, setzt Bank Frick auf ein umfassendes Business Continuity Management (BCM), das Strategien zur Aufrechterhaltung des Betriebs im Krisenfall umfasst. Notfall- und Wiederherstellungspläne für Wallets und digitale Vermögenswerte gewährleisten, dass selbst unerwartete Ausfälle keine lang anhaltenden negativen Auswirkungen haben. Durch gezielte Cybersecurity- und Incident-Response-Massnahmen kann auf potenzielle Sicherheitsbedrohungen reagiert werden.

Kontrollhandlungen und Verfahren

Zur Gewährleistung der Sicherheit der für Kund:innen verwahrten Kryptowerte wurden verschiedene Kontrollhandlungen und Verfahren implementiert. Dazu gehören insbesondere folgende Punkte:

- Bank Frick erfüllt die ISO-Norm 27001 zur digitalen Betriebsresilienz sowie alle Vorgaben der Verordnung (EU) 2022/2554 (DORA) zur Sicherstellung der digitalen Betriebsresilienz.
- Private Key Management (nur in Verbindung mit Kryptowerten): Bank Frick verwaltet die privaten Schlüssel, die für den Zugriff auf die Kryptowerte von Kund:innen nötig sind, mit höchster Sorgfalt und Vorsicht. Die privaten Schlüssel werden in einem sicheren Speicher aufbewahrt, der physisch und digital geschützt ist. Die privaten Schlüssel werden niemals an Dritte weitergegeben oder diesen gegenüber offengelegt. Die privaten Schlüssel werden nur von autorisierten Personen verwendet. Für die Speicherung der Private Keys und die Transaktionssignierung kommen Technologien wie MPC zum Einsatz.
- Transaktionsfreigabe: Bank Frick genehmigt von Warm und Cold Wallets ausgehende Transaktionen von Kryptowerten ausschliesslich nach einem strengen, definierten Verfahren. Für Mitarbeiter:innen, die Verfügungen aus Warm oder Cold Wallets vornehmen, gelten z. B. strenge Identitäts- und Zugangskontrollen. Transaktionen werden nur nach einer Mehrfaktor-Bestätigung durchgeführt, welche die Eingabe von PINs, Passwörtern, Codes und biometrischen Daten erfordert. Alle Transaktionen werden dabei von mehreren Personen überprüft und/oder freigegeben, die unterschiedliche Rollen und Verantwortlichkeiten haben. Die Transaktionen werden vor ihrer Ausführung zudem nach verschiedenen Kriterien wie Betrag, Häufigkeit, Empfänger:in und Risiko bewertet.
- Mitarbeiter:innen werden regelmässig geschult und für aktuelle Sicherheitsthemen sensibilisiert.
- Regelmässige externe und interne Audits gewährleisten eine kontinuierliche Sicherheitsbewertung der Systeme und Prozesse von Bank Frick. So können diese im Bedarfsfall angepasst werden.

Rechtliche Aspekte der Verwahrung

Trennung von Kryptowerten

Die im Rahmen der Verwahrung gehaltenen Kryptowerte verbleiben im Eigentum der jeweiligen Kund:innen und werden vermögensrechtlich, insbesondere in einem Insolvenz- oder Vollstreckungsverfahren, getrennt von den Kryptowerten von Bank Frick behandelt.

Allgemeine Geschäftsbedingungen

Bank Frick verwahrt die Kryptowerte für Kund:innen im Rahmen der Allgemeinen Geschäftsbedingungen einschliesslich des Depotreglements, welche auf der Webseite von Bank Frick abrufbar sind. Diese bilden einen integrierenden Bestandteil dieser Verwahrstrategie.