Informationen zu den verwendeten Sicherheitssystemen und der Verwahrstrategie

A. Verwahrstrategie

Die Tangany GmbH („**Tangany**“) erbringt im Rahmen ihrer Geschäftstätigkeit die Dienstleistung der Kryptoverwahrung (Verwahrung, Verwaltung und Sicherung von Kryptowerten und kryptografischen Instrumente und den dazugehörigen privaten Schlüsseln) sowie die Transferdienstleistung („**Verwahrdienstleistung**“) für den Kunden.

Tangany erbringt Verwahrdienstleistungen auf Grundlage von Kooperationsverträgen („**Kooperationsvertrag**“), die Tangany mit Kryptowerte-Dienstleistern, Betreibern von Krypto-Handelsplattformen und Händlern von Kryptowährungen („**Kooperationspartner**“) abschließt. Gemäß dem Kooperationsvertrag wird Tangany dafür vergütet, dass Tangany für Kunden des Kooperationspartner Verwahrdienstleistungen erbringt.

Die Verwahrstrategie von Tangany beschränkt sich allein auf die Verwahrung von Kryptowerten und kryptografischer Instrumenten für Kunden von Kooperationspartnern, damit diese Kooperationspartner Aufträge über Kryptowerte für ihre Kunden und sonstige Aufträge ausführen können.

Tangany verwahrt ohne Beteiligung von Kooperationspartner keine Kryptowerte und keine kryptografischen Insturmenten und plant dies auch nicht.

B. Verwendete Sicherheitssysteme

Die Tangany GmbH („**Tangany**“) hat die folgenden Vorkehrungen, Systeme und Verfahren („**Sicherheitssysteme**“) implementiert:

1. Sicherheitsvorkehrungen und Schutzmaßnahmen

Zur Verwahrung und Sicherung von Kryptowerten und kryptografischer Instrumenten kommen bei Tangany verschiedene Technologien zum Einsatz. Dazu gehören folgende Sicherungsmethoden:

a) Verwahrtechnologien

Multiparty Computation (MPC): Technologie zur Generierung, Speicherung und Nutzung kryptografischer Signaturschlüssel zum Schutz von Kryptowerten und kryptografischer Instrumente. 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 auf eine Teilmenge von Rechnern gelangen und wichtiges Material extrahieren können. Da jeder MPC-Teilnehmer die Transaktion richtliniengemäß überprüfen muss, ist es außerdem nicht möglich, die Schutzmaßnahmen zu umgehen, die zur Verhinderung des Missbrauchs eines Schlüssels installiert wurden.

Hardware Security Module (HSM): Dabei werden kryptografische Schlüssel in einer gesicherten Umgebung gespeichert. Der Signaturschlüssel kann nicht ausgelesen werden sondern nur für Signierzwecke genutzt werden. HSM sind ein fester Bestandteil der heutigen Bankeninfrastruktur.

b) Walletklassen

Cold Wallets: Krypto-Wallet, die nicht dauerhaft mit dem Internet verbunden ist. Es handelt sich um eine Infrastruktur, die im besonderen Maße geschützt und isoliert ist. Diese vornehmliche Offline-Speicherung macht Cold Wallets weniger anfällig für Online-Angriffe und bietet einen höheren Sicherheitsgrad für Kryptowerte und kryptografischer Instrumenten.

Warm Wallets: Krypto-Wallets, die für die Interaktion mit anderen Anbietern genutzt werden. Dazu gehört etwa der Händler (Kauf und Verkauf von Kryptowährungen). Die Wallets zeichnen sich durch einen höheren Grad an Automatisierung aus.

2. Trennung zwischen den Kryptowerten und kryptografischer Instrumenten der Kunden und Tangany eigenen Kryptowerten

Die von Tangany verwahrten Kryptowerte und kryptografischer Instrumente der Kunden werden streng operativ getrennt von Tangany eigenen Kryptowerten und kryptografischer Instrumenten verwahrt. Kundeneigene Kryptowerte und kryptografische Instrumente gelten stets den Kunden zugehörig, dieser ist Eigentümer der Kryptowerte und kryptografischen Instrumente.

Zur Sicherstellung der Trennung werden die Kryptowerte und kryptografischen Instrumente der Kunden in Sammelverwahrung verwahrt. Für jede Plattform wird für die Kunden eine eigene Omnibus-Wallet eingerichtet, auf der die Kryptowerte bzw. kryptografischen Instrumente der Kunden der Plattform zusammen verwahrt werden. Die Zuordnung des Eigentums der Kunden an den Kryptowerten bzw. kryptografischen Instrumente der Omnibus-Wallet findet über ein internes Buchhaltungssystem statt.

Im Fall einer Insolvenz von Tangany sind die Kryptowerte und kryptografischen Instrumente somit eindeutig dem Kunden zuzuordnen und durch den Insolvenzverwalter aussonderungsfähig.

Tangany nutzt ohne Zustimmung der Kunden deren Kryptowerte und kryptografischen Instrumente nicht für andere Zwecke, um diese z.B. zu verleihen oder zu staken.

Mitarbeiter von Tangany sind nicht befugt, sich Eigentum oder Besitz an von Tangany verwahrte Kundenkryptowerten und -kryptografischen Instrumente zu verschaffen.

3. Notfall- und Wiederherstellungspläne

Tangany verfügt über Notfall- und Wiederherstellungspläne für die unter Ziffer 1 genannten Verwahrlösungen. Gleichzeitig existiert ein Notfallplan für die Wiederherstellung des internen Buchungssystems, über das die Kundenbestände eindeutig den Kunden zuordenbar sind. Die Pläne werden im regelmäßigen Abstand auf ihre Aktualität geprüft und bei Bedarf angepasst.

4. Transparenzanforderungen

Tangany ist als Kryptoverwahrer verpflichtet, seinen Kunden mindestens alle drei Monate und auf Verlangen über ihre bei Tangany verwahrten aktuellen Kryptowerte-Positionen zu berichten. Diese Berichte stellt Tangany den Kunden kostenlos zur Verfügung.

Tangany ist nicht verpflichtet, an Ereignissen der zu Grunde liegenden DLT teilzunehmen, die neue Rechte für den Kunden begründen. Ein Ereignis könnte z.B. ein “Hard Fork” sein, bei dem die betreffende Blockchain sich in ein oder mehrere Teile aufspaltet, und neue Kryptowerte generiert werden. Als weiteres Beispiel können "Airdrops" aufgeführt werden, bei denen es zu einer Zuteilung von neuen Kryptowerten auf die Omnibus-Wallet der Plattform kommen kann. Eine Zuteilung auf einzelne Kundenkonten ist in diesem Fall nicht möglich.

Auf Risiken in der Kryptowerwahrung wird gesondert im Bereich “Information zu Risiken in der Kryptoverwahrung und Transferdienstleistungen” hingewiesen.

Informationen zu Preisen und Gebühren sind im “Preis- und Leistungsverzeichnis” aufgeführt.

5. Risikomanagement und Kontrollverfahren

Tangany hat umfassende Strategien und Verfahren implementiert, um den sicheren Umgang mit Kryptowerten und kryptografischer Instrumenten zu gewährleisten und Risiken gezielt zu minimieren. Im Einzelnen umfassen die Kontrollmechanismen folgende Maßnahmen:

a) Informationssicherheitssystem

Ein strukturiertes Informations- sicherheitssystem stellt die Einhaltung der Schutzbedarfsziele Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität sicher. Regelmäßige Risikoanalysen und Bedrohungsbewertungen sind zentrale Bestandteile, um die Kontinuität und Verlässlichkeit der technischen und organisatorischen Sicherheitsvorkehrungen zu gewährleisten.

b) Sicherer Softwareentwicklungszyklus

Unsere Produkte werden in einem sicheren Softwareentwicklungszyklus (Secure Software Development Lifecycle, SSDLC) entwickelt. Durch die Integration von Sicherheitskontrollen in jeder Entwicklungsphase sollen Sicherheitsrisiken frühzeitig erkannt und minimiert werden.

c) Technische Schutzmaßnahmen zur Infrastruktur

Der Betrieb unserer technischen Infrastruktur wird durch eine Reihe von Schutzmaßnahmen abgesichert. Dazu gehören Firewalls, Verschlüsselungstechnologien, Zugriffskontrollen und kontinuierliche Überwachungen, die eine frühzeitige Erkennung und Reaktion auf sicherheitsrelevante Ereignisse ermöglichen.

d) Interne Sicherungsmaßnahmen und Vier-Augen-Prinzip

Sicherheitsrelevante Vorgänge werden durch interne Sicherungsmaßnahmen und das Vier-Augen-Prinzip unterstützt. Diese Vorgehensweise gewährleistet, dass sicherheitskritische Aktionen von mindestens zwei autorisierten Personen überprüft werden, um Fehler und potenzielle Missbrauchsrisiken zu vermeiden.

e) Regelmäßige Schulung der Mitarbeiter

Mitarbeiter werden regelmäßig geschult und für aktuelle Sicherheitsthemen sensibilisiert. Diese Schulungen umfassen bewährte Methoden im Umgang mit Kryptowerten und kryptografischer Instrumenten und Anpassungen an neue Bedrohungslagen und Sicherheitsanforderungen.

f) Regelmäßige Prüfung des internen Kontrollsystems

Das interne Kontrollsystem (IKS) wird kontinuierlich geprüft, um die Wirksamkeit und Einhaltung aller Sicherheitsrichtlinien und -verfahren sicherzustellen. Interne und externe Prüfungen dienen dazu, bestehende Schutzmaßnahmen zu evaluieren und bei Bedarf anzupassen.

6. Transaktions-Monitoring

Tangany prüft und überwacht Transfers von Kryptowerten und kryptografischer Instrumenten gesamtheitlich während und nach Ausführung des Transfers risikobasiert nach definierten Kriterien, die regelmäßig überprüft und - falls erforderlich – angepasst werden. Zur Einhaltung dieser Anforderungen werden Daten- analysesysteme eingesetzt, die auf aktuelle und historische Kundentransfers zurückgreifen und nach festgelegten Regeln die Transferdaten der Kunden analysieren.