Conio Srl	**Predisposta da:** Funzione di Controllo
	Versione di: Maggio 2026
Stato	**Approvato dal** Consiglio di Amministrazione in data 15/06/2026

SINTESI
POLITICA DI CUSTODIA

Premessa

Conio s.r.l. (di seguito "**Conio**" o la "**Società**"), da sempre attenta alle esigenze dei propri clienti, alle cui esigenze presta massima attenzione per garantirne la soddisfazione, consolidare la fiducia e tutelare la propria reputazione. In conformità a quanto previsto dalla normativa primaria e secondaria di recepimento del Reg. Ue n. 2023/1114 (di seguito, per brevità, "**MiCAR**"), Conio ha predisposto una politica di custodia e amministrazione (di seguito la "**Policy**") contenente una descrizione delle modalità operative volte a garantire la separazione del patrimonio della Società dai beni riconducibili ai clienti di Conio nell'ambito della prestazione dei servizi.

L'utilizzo da parte di Conio di ciascun servizio menzionato nel presente documento è subordinato all'ottenimento, da parte del rispettivo prestatore di servizi per le cripto-attività, delle autorizzazioni necessarie ai sensi del Regolamento MiCA. Conio si impegna a verificare preventivamente il possesso di tali requisiti prima di usufruire del servizio.
Il presente documento (di seguito la "Sintesi") rappresenta una sintesi di cinque policy – nello specifico: (i) politica di custodia e amministrazione; (ii) politiche per la segregazione delle cripto-attività; (iii) politica sulla tutela dei fondi dei clienti; (iv) politica di gestione delle chiavi crittografiche; ~~e~~ (v) digital asset custody risk management policy – ed è messo a disposizione dei clienti di Conio, i quali possono richiederne una copia inviando una email al seguente indirizzo: support@conio.com

Ai fini della presente Sintesi, valgono le seguenti definizioni:

- **Cripto-attività**: una rappresentazione digitale di un valore o di un diritto che può essere trasferito e memorizzato elettronicamente, utilizzando la tecnologia a registro distribuito o una tecnologia analoga (MICAR, art. 3(1)(5));
- **Cliente**: qualsiasi persona fisica o non fisica che ha completato l'intero processo di onboarding, compilato il Questionario antiriciclaggio, e superato con esito positivo la fase di verifica dell'identità, della veridicità e correttezza delle informazioni e dei documenti forniti e conseguentemente può beneficiare del Servizio;
- **Fondi**: valuta avente corso legale;
- **Servizio**: il servizio di custodia e amministrazione di cripto-attività, inteso come la custodia o il controllo, per conto di clienti, delle cripto-attività o dei mezzi di accesso a tali cripto-attività, se del caso sotto forma di chiavi crittografiche private.
- **MiCAR (Markets in Crypto-Assets Regulation)**: Il Regolamento (UE) 2023/1114, che stabilisce un quadro normativo per i mercati delle cripto-attività.
- **Cold Wallet**: Portafogli mantenuti completamente offline al fine di garantire la massima protezione da rischi come attacchi informatici o problemi tecnici delle piattaforme online.

- **Hot Wallet**: Portafogli online, come quelli dei prestatori di servizi in cripto-attività (es. Coinbase e Kraken)
- **Multisig (Multi-firma)**: Tecnologia che richiede l'approvazione di più firmatari autorizzati per eseguire transazioni, garantendo maggiore sicurezza.
- **MPC (Multi-Party Computation)**: Tecnologia che garantisce che le chiavi private non siano accessibili a una singola parte, aumentando la sicurezza, e utilizzata per la generazione e divisione della terza chiave.
- **TEE (Trusted Execution Environment)**: Ambienti di esecuzione sicuri dove viene generata e conservata la seconda chiave di Conio, assicurando che la chiave rimanga crittografata durante tutto il suo ciclo di vita.
- **Gestore di piattaforma di negoziazione**: il gestore di uno o più sistemi multilaterali che consente o facilita l'incontro, all'interno del sistema e in base alle sue regole, di molteplici interessi di terzi per l'acquisto o la vendita di cripto-attività, in modo tale da portare alla conclusione di contratti, scambiando cripto-attività con fondi, o scambiando cripto-attività con altre cripto-attività;

La Policy viene predisposta dalla funzione di Finanza e Controllo ed è approvata dal Consiglio di amministrazione, responsabile della sua corretta attuazione; è soggetta a revisione periodica anche in considerazione degli eventuali aggiornamenti di tempo in tempo necessari.

È responsabilità delle funzioni aziendali coinvolte segnalare all'amministratore delegato o alla funzione Risk Management, eventuali criticità e proporre intervento migliorativi e modificativi; le funzioni Finance e Controllo e l'area Risk Management della Funzione di Controllo, invece, provvedono a monitorare l'evoluzione normativa esterne o interne in caso di cambiamenti nella struttura organizzativa, segnalando tempestivamente la necessità di adeguamenti.
A seguire, vengono disciplinati diversi aspetti, e specificatamente:

(I) Presidi organizzativi e contrattuali

(i) sistemi di custodia e controllo

Per la custodia delle cripto-attività Conio adotta un approccio multilivello con l'obiettivo di mitigare i rischi operativi, di sicurezza e di controparte.

Le modalità di segregazione delle cripto-attività e dei fondi dei clienti sono dettagliatamente descritte all'interno delle **politiche per la Segregazione delle Cripto-Attività e dei Fondi dei Clienti** (Cfr. Allegato n.35), e all'interno della **politica sulla tutela dei fondi dei clienti** (Cfr. Allegato 51), concernente i presidi organizzativi di Conio volti a garantire la separazione patrimoniale dei fondi e delle cripto-attività riconducibili al cliente, per tutelare i diritti di titolarità dei Clienti (anche in ipotesi di insolvenza della Società) e prevenire l'uso dei fondi dei Clienti per conto proprio.

Più nel dettaglio, in tali Politiche sono disciplinati:

- ***i presidi generali***

Conio, in particolare, tutela le disponibilità dei clienti in cripto-attività e fondi (cfr. Policy Tutela Fondi). Le cripto-attività e i fondi sono di proprietà dei Clienti e restano di proprietà dei Clienti anche quando vengono

trasferite o trasmesse alla Società per l'accesso ai Servizi o alle funzionalità degli stessi. La Società non utilizza, investe o impiega, per fini diversi dal servizio di scambio di cripto-attività con fondi o altre cripto-attività, di collocamento e di custodia di cripto-attività, i fondi o le cripto-attività dei Clienti. I fondi e le cripto-attività costituiscono patrimonio distinto e separato a tutti gli effetti da quello della Società.

- ***i presidi speciali – politiche di segregazione:***

a. ***Garanzie di Separazione Patrimoniale****: C*onio adotta un approccio rigoroso per garantire che le risorse dei clienti siano sempre protette e non vengano mai utilizzate per scopi propri della Società. Questo impegno si articola nei seguenti principi operativi:

i) *Divieto di utilizzo dei fondi dei clienti*: i fondi depositati dai clienti (in valuta tradizionale o fiat) sono mantenuti separati dal capitale operativo di Conio e non vengono mai impiegati per coprire spese aziendali, finanziare operazioni proprie o per qualsiasi altra attività diversa dalle istruzioni dei clienti stessi. I fondi depositati dai clienti sono mantenuti in un conto corrente segregato, il cui accesso dispositivo è limitato ai dipendenti con delega del CEO della Società. La movimentazione del conto è automatica, attraverso l'uso di API (Application Program Interface) la cui chiamata è strettamente legata alle attività dei clienti. Gli interventi manuali sul conto sono legati unicamente a sporadiche correzioni da effettuare.

ii) *Separazione delle cripto-attività*: le cripto-attività dei clienti sono custodite in strutture digitali completamente distinte dalle risorse proprie della Società. Le cripto-attività sono custodite per conto dei clienti in via prevalente su Kraken custody in cold wallet, , che, al fine di garantire la massima protezione del capitale da rischi utilizza la tecnologia MPC (Multi-Party Computation) che fornisce presidio contro smarrimento/distruzione della chiave privata e il robusto protocollo di air-gapping per la soluzione di cold storage fornita a Conio, garantendo che i dispositivi contenenti il materiale crittografico non siano mai esposti a reti pubbliche. Per casi al di fuori dell'operatività ordinaria, quali manutenzioni temporanee, aggiornamenti infrastrutturali, interruzioni impreviste delle API dei partner primari o contesti di Business Continuity, Conio si riserva la possibilità di allocare una porzione residuale (tra lo 0,01% e il 5%) dei fondi sul wallet omnibus di Coinbase per intervalli temporali transitori e strettamente limitati alla durata dell'evento eccezionale, garantendo così la continuità del servizio di scambio per la clientela.

iii) *Distinzione dei wallet:* i wallet omnibus contenenti le cripto-attività dei clienti hanno credenziali di accesso diverse rispetto ai wallet contenenti le cripto-attività di Conio, riducendo al minimo il rischio di errori operativi o utilizzi non autorizzati. Sono predisposti audit periodici, che assicurano che la separazione patrimoniale sia sempre rispettata.

b. ***una descrizione dettagliata del sistema di approvazione per le chiavi crittografiche e di garanzia di queste (per es. dei wallets multi-firma)***

Conio adotta un approccio multilivello per la custodia delle cripto-attività, con l'obiettivo di mitigare i rischi operativi, di sicurezza e di controparte. La custodia di Conio è basata su una tecnologia robusta secure-by-design multifirma che combina tecnologie multisig native e multiparty computation (MPC) con chiavi warm e cold. Le sue procedure si basano su una custodia diversificata. Su tre chiavi totali, ogni cliente

detiene il controllo di una delle chiavi private del proprio wallet on-chain, non accessibile né da Conio né a terze parti; la seconda chiave è detenuta da Conio ed è necessaria per autorizzare le operazioni del wallet del cliente. Ogni transazione richiede la controfirma con questa chiave, attivabile dal cliente tramite un codice di autenticazione a due fattori (2FA); la terza chiave, infine, è in custodia presso un ente terzo indipendente a Conio, e può essere utilizzata solo in caso di richiesta da parte del cliente di recupero dei fondi. Per la descrizione delle 3 chiavi (e wallet utente - wallet aziendali) si veda *infra*.

c. ***Modalità di Segregazione***

Le cripto-attività dei clienti sono custodite in strutture digitali completamente distinte dalle risorse proprie della Società. Conio non utilizza tali cripto-attività per trading proprietario, lending o altre attività speculative. Per garantire massima flessibilità e sicurezza, Conio prevede due distinte modalità di detenzione per i clienti:

- Custodia Diretta (Wallet On-Chain): per blockchain bitcoin, i clienti detengono i fondi direttamente su wallet multi-firma (multisig) di cui possiedono una delle chiavi private.
- Custodia Fiduciaria (Sistema Ledger Interno e Wallet Omnibus): per altri asset, i clienti detengono token rappresentativi registrati su una blockchain privata interna a Conio, che traccia in modo immutabile la proprietà. Il controvalore reale di queste cripto-attività è custodito da Conio in conti aggregati (omnibus), mantenuti separati dal patrimonio aziendale e allocati per la maggior parte in cold wallet presso custodi terzi istituzionali, segregati dalle cripto-attività del custode terzo e degli altri clienti del custode (es. Kraken Custody), o in wallet gestiti direttamente da Conio stessa. L'infrastruttura di custodia per i wallet omnibus si avvale di partner istituzionali esterni.
  Sebbene i fondi dei clienti Conio siano aggregati in questi portafogli, la segregazione patrimoniale è garantita a livello di provider:

    - Conti Omnibus presso Custode Primario (Kraken Custody): Conio custodisce la stragrande maggioranza dei fondi aggregati dei clienti in questi wallet (cold wallets). In questi conti, il patrimonio dei clienti Conio è separato non solo da quello di Conio stessa, ma anche dal patrimonio del provider terzo (Kraken) e da quello degli altri clienti del provider. Questo annulla il rischio di controparte in caso di insolvenza del provider.

- Conti Omnibus presso Fornitori Secondari (Coinbase): Utilizzati in via residuale e temporanea per garantire l'operatività (es. liquidità per scambi, hot wallet), le manutenzioni o in scenari di Business Continuity.

- *Segregazione dei fondi fiat*: per i fondi in valuta tradizionale, ogni cliente dispone di un IBAN dedicato, associato a un conto segregato intestato alla Società ma riservato esclusivamente alle risorse dei clienti. Ciò garantisce la separazione patrimoniale e impedisce qualsiasi commistione con i fondi aziendali. Queste modalità sono integrate da processi di monitoraggio continuo, che verificano l'integrità delle risorse e la corretta applicazione delle politiche di segregazione.

d. Deposito dei Fondi dei Clienti

La gestione dei fondi fiat dei clienti segue regole precise per garantire tempestività e sicurezza: (i) i fondi ricevuti dai clienti vengono depositati presso istituti di credito autorizzati entro la fine del giorno lavorativo successivo alla loro ricezione, con un processo automatizzato per ridurre i tempi di elaborazione e minimizzare i rischi operativi; (ii) una volta accreditati o prelevati dalla posizione in euro del cliente, il sistema di Conio esegue le operazioni in tempo reale, rispettando i tempi di regolamento bancario standard (ad esempio, bonifici SEPA). Se i fondi rimangono nella posizione in euro del cliente, sono immediatamente disponibili per operazioni di compravendita, garantendo liquidità e flessibilità agli utenti. (iii) i conti bancari utilizzati per i fondi dei clienti sono distinti da quelli aziendali e identificati con denominazioni specifiche, che ne evidenziano la natura segregata. Questa chiarezza nella titolazione facilita la supervisione da parte delle autorità regolamentari e rafforza la fiducia degli utenti.

e. Criteri di Selezione degli Istituti di Credito

Qualora Conio non depositi i fondi presso una banca centrale, la scelta degli istituti di credito si basa su criteri rigorosi e ben definiti: (i) stabilità finanziaria/patrimoniale, valutata attraverso rating creditizi e analisi dei bilanci; (ii) conformità normativa, istituzioni devono essere autorizzate e conformi alle normative locali ed europee (es. Direttiva PSD2, Regolamento MiCAR) per essere considerati partner accettabili; (iii) revisione periodica, la selezione degli istituti viene riesaminata ogni sei mesi, con una valutazione documentata che considera fattori come performance operativa, feedback di mercato e cambiamenti normativi. Questo processo è supportato da una politica interna sulla diversificazione, che viene aggiornata annualmente per riflettere le condizioni di mercato. Conio si affida a Banca Sella S.p.A. per la gestione dei fondi in valuta fiat depositati dai clienti. Gli IBAN dedicati a ciascun cliente non corrispondono a conti di pagamento intestati direttamente al cliente, bensì a IBAN virtuali riconducibili a conti di pagamento segregati intestati a Conio presso Banca Sella, ma utilizzati esclusivamente per le disponibilità dei clienti, in piena conformità con la normativa applicabile in materia di segregazione patrimoniale.

f. Presidi contrattuali

La Società precisa nel contratto di prestazione dei servizi con i clienti che i fondi e le cripto-attività sono e restano di proprietà dei clienti stessi. Nei contratti con gli istituti di credito, per il deposito dei fondi dei Clienti funzionali alla prestazione dei Servizi, Conio avrà cura di precisare che i fondi che transitano su quel conto sono di proprietà dei clienti. È poi chiarito che sul conto utilizzato da Conio per tale operatività non sono ammesse azioni da parte dei creditori della Società o nell'interesse degli stessi, né dei creditori degli istituti di credito.

g. Scenario di stress

Questi criteri assicurano che i fondi dei clienti siano depositati in ambienti sicuri e affidabili, mantenendo la continuità operativa anche in scenari di stress finanziario.

h. Criteri di Selezione dei prestatori di servizi in cripto-attività e Custody Provider

Conio in via prudenziale tratta i prestatori di servizi in cripto-attività presso cui si approvvigiona per la fornitura del servizio di custodia e amministrazione e quello di scambio come delegati. I due principali fornitori sono: Kraken, Coinbase (*infra*, "*sistema di custodia, delega di custodia a terzi e liquidity provider").*

- **monitoraggio sul presidio organizzativo relativo alla separazione patrimoniale**

La funzione Amministrazione Finanza e Controllo di Conio controlla annualmente l'efficacia dei presidi organizzativi di separazione patrimoniale in modo da identificare e, se del caso, correggere eventuali carenze. La funzione presenta le risultanze della verifica all'amministratore delegato o alla Funzione Unica di Controllo per le valutazioni del caso.

- **informativa cliente**

Conio si impegna a comunicare ai clienti le proprie politiche di segregazione e custodia in modo chiaro, conciso e accessibile nell'ambito della sintesi delle politiche di custodia, evitando tecnicismi che potrebbero risultare incomprensibili. Questo impegno si concretizza altresì attraverso: (i) *canali di comunicazione*: tramite una sezione dedicata all'interno delle F.A.Q. presente sul sito web di Conio (identificata come "Custodia dei fondi e Sistema di Recupero") fornisce una panoramica aggiornata delle misure adottate, mentre la documentazione contrattuale (es. Termini e Condizioni) include dettagli specifici sulle garanzie offerte; (ii) *reportistica*: i clienti ricevono un rendiconto trimestrale dettagliato sulle loro cripto-attività e fondi custoditi, con informazioni sulla quantità, tipologia e modalità di custodia. Inoltre, possono richiedere estratti conto elettronici in qualsiasi momento tramite l'app o il portale web; (iii) *linguaggio accessibile*: le informazioni sono redatte in conformità con l'articolo 70, paragrafi 1, 2 e 3, del Regolamento (UE) 2023/1114, utilizzando un linguaggio semplice e diretto, con esempi pratici; (iv) aggiornamenti regolari: i clienti vengono informati tempestivamente di eventuali modifiche alle politiche tramite notifiche push o e-mail, garantendo una trasparenza costante.

La descrizione delle modalità operative di gestione delle chiavi crittografiche e del loro ciclo di vita si trova all'interno della **politica di gestione delle chiavi crittografiche** (Cfr. Allegato n.50) predisposta dalla funzione di ICT ed approvata dal Consiglio di amministrazione, il quale è responsabile della sua corretta attuazione; Tale politica ha lo scopo di evitare che alcuna parte coinvolta sia in possesso di sufficienti privilegi per operare in autonomia sui fondi. Specificatamente, in tale politica vengono disciplinati i seguenti aspetti:

a. La gestione delle Chiavi e Ciclo di Vita nella Custodia di Conio

Il sistema di gestione delle chiavi crittografiche è strutturato per garantire massima sicurezza e protezione dei beni digitali dei clienti, obiettivi che rappresentano priorità assoluta per Conio.
A tal fine, Conio opera con un'architettura di custodia con un approccio multilivello basato su una tecnologia multifirma "secure-by-design" che integra soluzioni "multisig" native e la "multi-party computation" (MPC) con un sistema di gestione delle chiavi che include sia chiavi "warm" che "cold", in moda da mitigare efficacemente i rischi operativi, di sicurezza e di controparte, garantendo la massima protezione e disponibilità dei fondi dei clienti. Le chiavi che gestiscono il portafoglio multisig sono intrinsecamente "on-chain", ereditando, così, le robuste garanzie crittografiche intrinseche della blockchain stessa. Le tre chiavi essenziali per l'operatività sono generate e detenute da tre parti distinte per l'intero ciclo di vita, minimizzando così in modo significativo i rischi di compromissione o di accesso non autorizzato.

b. Le tre chiavi

1. Chiave del cliente (Prima Chiave)

La gestione della "Chiave del Cliente" rappresenta il primo e più diretto livello di controllo sulla sicurezza delle cripto-attività detenute con Conio. La Società ha progettato un sistema in cui la proprietà e il controllo di questa chiave rimangono saldamente nelle mani del cliente.

Per quanto riguarda la generazione della chiave, la soluzione di integrazione di Conio è basata sull'utilizzo di una SDK integrata nell'app, in grado di colloquiare con il backend di Conio.

Al momento della *Signup*, in cui il cliente decide di iscriversi al wallet di Bitcoin, questa SDK genera la chiave privata del cliente, la User Key. Il processo prevede tre passaggi principali: (i) l'SDK genera una sequenza random di 12 parole (Mnemonic Key) secondo le specifiche BIP39, da cui si definisce un SEED; (ii) dal SEED, l'SDK deriva la chiave privata del cliente (User Private Key) secondo le specifiche BIP32; (iii) dalla chiave privata l'SDK deriva la chiave pubblica del cliente (User Public Key).

Per garantire la massima protezione, la Mnemonic Key e la User Private Key vengono cifrate con la password del cliente e salvate nel secure storage del dispositivo mobile. Vengono inoltre cifrate e salvate anche sul backend di Conio, così da garantire il recupero delle informazioni in caso di smarrimento o cambio dispositivo; Il backend di Conio infatti, ogni volta che un cliente dall'app richiama la procedura di login, rimanda al device la Mnemonic Key e la User Private Key cifrate. In questo modo, se il cliente ha cambiato smartphone, l'SDK potrà salvare nel secure storage le informazioni criptate e decifrarle alla bisogna attraverso la password. La User Public Key, invece, è salvata in chiaro sul backend di Conio. Questa struttura permette di evitare che, anche in caso di accesso fraudolento al secure storage, sia possibile ricostruire in chiaro le chiavi del cliente.

L'app stessa salva nel secure storage informazioni dei clienti (chiavi private) cifrate con un segreto (password), per cui pur accedendo in modo "fraudolento" al secure storage non c'è modo di impadronirsi delle componenti in chiaro delle chiavi del cliente.

Dal punto di vista della sicurezza, questa chiave è classificata come "warm" perché, per poter firmare una transazione, deve essere sbloccata tramite biometria o PIN, oltre a un secondo fattore di autenticazione (2FA) mediante SMS o applicazione Authenticator. L'accesso ai fondi custoditi avviene da parte dei clienti tramite un'app, che impone l'autenticazione a più fattori (MFA) per prevenire accessi non autorizzati.
Nel ciclo di vita delle transazioni, il cliente è responsabile della firma utilizzando la propria chiave privata. Dopo la firma, la transazione viene inoltrata ai sistemi di Conio per la verifica.

2. Chiave di Conio (seconda chiave)

La "Chiave di Conio" costituisce un elemento cardine dell'architettura di sicurezza di Conio, agendo come co-firmatario essenziale nelle operazioni sui wallet dei clienti.

Per quanto riguarda la generazione della chiave, questa avviene e viene conservata nei Trusted Execution Environment (TEE) del cloud di Conio, tuttavia, nessuno nessun dipendente di Conio può accedere direttamente a questa chiave nel suo intero ciclo di vita. All'interno dello stesso TEE, la chiave di Conio viene utilizzata per derivare le singole chiavi private di Conio, ognuna associata a ciascun indirizzo degli utenti, in conformità con le specifiche del protocollo BIP32 di Bitcoin. Anche questa chiave è considerata "warm", poiché i sistemi di firma di Conio sono condizionati da controlli "off-chain", come permessi di invio e limiti

predefiniti. La natura stessa del TEE assicura che la chiave resti sempre crittografata durante tutto il suo ciclo di vita.

La chiave di Conio può essere utilizzata esclusivamente per firmare transazioni blockchain tramite i sistemi di firma di Conio. Ogni transazione richiede due firme per essere autorizzata: quella del cliente e quella di Conio. Una volta che l'utente firma una transazione, questa viene inoltrata ai sistemi di Conio che provvedono a verificarla. Se le verifiche hanno esito positivo, Conio controfirma la transazione utilizzando la propria chiave e successivamente la inoltra sulla blockchain.

3. Chiave del partner (terza chiave)

La terza chiave rappresenta una salvaguardia esterna fondamentale; per quanto riguarda la sua generazione, il primo passaggio è la cerimonia di creazione della chiave di backup. La cerimonia prevede che N persone (Key Custodian) inseriscano ciascuno un proprio pezzo di chiave all'interno di una procedura per generare la chiave privata di backup e la corrispondente chiave pubblica. Contestualmente, viene definito il quorum (M) di chiavette necessario per ricostruire la Backup Key. Si evince quindi che $1<M<=N$.

I Key Custodian non digitano manualmente un segmento di chiave, ma utilizzano dispositivi HSM (Hardware Security Module) dedicati, uno per ogni Key Custodian. L'hardware scelto per questa soluzione è l'USB Armory di F-Secure (https://inversepath.com/usbarmory).

Le *N* USB Armory (di seguito la "chiavetta") vengono inizializzate distribuendo su di esse lo stesso certificato, così da generare un pool univoco comune. Una volta creato il pool delle N chiavette, non sarà possibile aggiungere nuove chiavette al pool.

A questo punto, i Key Custodian, inseriscono, scegliendo una finestra temporale in cui sono tutti disponibili, le USB Armory nei propri PC e avviano la procedura di generazione della Backup Key scegliendo una propria password da associare alla propria chiavetta che ha lo scopo di proteggere le varie HSM dall'utilizzo non autorizzato di altre persone all'infuori di loro. Una volta completata la procedura, una chiave privata (Backup Private Key) viene generata automaticamente e distribuita in parti sulle chiavette. Il pool di chiavette deriva poi una chiave pubblica della chiave privata (Backup Public Key), che verrà comunicata a Conio il quale la utilizzerà per la creazione degli indirizzi HD multisig di ciascun cliente. La Backup Private Key non può mai essere visualizzata in chiaro da alcuna persona.

Dal punto di vista della natura e requisiti di sicurezza, questa chiave è da considerarsi "cold", in quanto conservata offline, minimizzando così i rischi di compromissione online. La frammentazione e distribuzione tramite MPC ne aumenta intrinsecamente la sicurezza.

La terza chiave può essere utilizzata solo in caso di richiesta del cliente per esigenze di recupero fondi; la procedura di recupero di Conio prevede l'utilizzo della terza chiave tramite l'apposita procedura di recovery. Pertanto, un quorum M-di-N delle terze parti dovrà firmare una transazione (dopo gli opportuni controlli) unitamente alla chiave di Conio per movimentare i fondi su un nuovo portafoglio.

(ii) identificazione delle Cripto-Attività e dei Mezzi di Accesso

Le cripto-attività custodite per conto dei clienti sono tracciate e identificate attraverso un sistema di registrazione su blockchain privata. Ogni transazione e saldo è registrato su una blockchain privata,

utilizzando indirizzi univoci e verificabili. Le attività dei clienti sono conservate in wallet dedicati, separati da quelli aziendali, per evitare qualsiasi commistione di fondi, e ogni cliente è associato a un identificativo univoco, che permette di collegare le allocazioni delle cripto-attività su wallet aziendali, prestatori di servizi in cripto-attività e servizi di custodia terzi.

Per garantire l'accuratezza dei dati, l'azienda effettua una riconciliazione mensile tra i saldi contabili interni e i saldi reali su blockchain e rispetto agli altri prestatori di servizi in cripto-attività, qualsiasi discrepanza attiva immediatamente allarmi, si innesca un processo di indagine e risoluzione.

I mezzi di accesso alle cripto-attività variano in base alla tipologia di custodia: per i fondi custoditi su wallet omnibus gestiti direttamente da Conio, Kraken Custody e Coinbase le credenziali di accesso sono protette da vault crittografato e autenticazione a due fattori (TOTP). Inoltre, è stata implementata una whitelist di indirizzi per i prelievi, limitando le operazioni a indirizzi pre-approvati.

Per i clienti che utilizzano il proprio wallet, i mezzi di accesso (chiavi private) sono sotto il controllo dell'utente. L'azienda non conserva né accede a queste chiavi, garantendo autonomia e sicurezza dei propri fondi. Per le altre cripto-attività, l'accesso dei clienti avviene tramite app su smartphone, con obbligo di autenticazione a più fattori (MFA) per prevenire accessi non autorizzati.

(iii) sistema di custodia, delega di custodia a terzi e liquidity provider

Conio prevede un sistema di custodia e amministrazione on chain (i.e. wallet Bitcoin on-chain) e off chain. Nell'ambito di tale attività, Conio può anche avvalersi di fornitori terzi che attualmente sono: Coinbase e Kraken, Bitstamp (Bitstamp solo per la custodia e amministrazione di asset di proprietà di Conio).

Per le cripto-attività in cui la custodia e amministrazione è on-chain (i.e. wallet Bitcoin on-chain) Conio non si avvale di fornitori terzi, mentre per le cripto-attività che il cliente non detiene direttamente sul proprio wallet on-chain, ma attraverso il possesso di un token che le rappresenta su una blockchain privata (i.e. off-chain), la custodia e amministrazione delle cripto-attività avviene, in parte, attraverso i fornitori sopra menzionati, utilizzati sia come fornitori di liquidità sia come delegati da Conio alla custodia di cripto-attività dei clienti.

Conio, in via prudenziale, tratta tutti i prestatori di servizi in cripto-attività come fossero delegate, applicando quindi le politiche di selezione del fornitore. I principali prestatori di servizi in cripto-attività di cui si avvale Conio sono Kraken e Coinbase. (cfr. *infra*)

Per quanto riguarda i conflitti di interesse, l'azienda adotta politiche rigorose per garantire trasparenza e imparzialità. Non viene effettuato trading proprietario con i fondi clienti, né sono previsti accordi di revenue sharing con i fornitori esterni. Le commissioni di transazione sono fisse, assicurando che gli interessi dei clienti siano sempre prioritari (si veda, policy conflitti). Il monitoraggio delle attività delegate è garantito attraverso strumenti di controllo avanzati e procedure strutturate. Inoltre, audit esterni trimestrali sono condotti da società indipendenti, per verificare l'aderenza agli SLA e la conformità alle normative vigenti.
Sono stati implementati parametri di allerta per identificare tempestivamente eventuali anomalie e, infine, si evidenzia che l'azienda effettua una revisione contrattuale annuale dei fornitori, aggiornando gli SLA in base ai cambiamenti normativi (ad esempio, MiCA o DORA) e alle performance storiche dei fornitori.

Quanto al processo di selezione e monitoraggio dei fornitori (prestatori di servizi in cripto-attività) per attività di liquidity provider e custodia e amministrazione, all'interno della Policy viene disciplinata la delega di funzioni a terzi secondo due principi:

- principi di delega, che specificano criteri e condizioni per l'affidamento di attività di custodia a fornitori terzi qualificati;
- limitazione delle finalità, secondo cui la delega è consentita unicamente per le finalità specifiche descritte nella politica, escludendo qualsiasi attività non menzionata.

Conio adotta un processo strutturato e prudenziale per la selezione dei prestatori di servizi in cripto-attività. I fornitori attualmente attivamente utilizzati, nel rispetto delle policy interne e delle normative applicabili, sono:

1. Coinbase: ha ottenuto la licenza come CASP in Lussemburgo ed è Regolamentata come EMI e VASP in Irlanda e abilitata in più giurisdizioni UE. le funzioni delegate sono quelle di custodia e liquidity provider, con esecuzione di operazioni di trading crypto-to-euro con elevata liquidità e profondità di book
2. Kraken: ha ottenuto la licenza CASP in Irlanda ed è regolamentata come EMI e VASP, nonchè autorizzata per i derivati crypto; le funzioni delegate sono quelle di custodia e liquidity provider e presta supporto tecnico avanzato tramite API;

Sono scelti in base a criteri stringenti, tra cui: (i) regolarità autorizzativa; (ii) compatibilità con le coppie di scambio in euro; (iii) profondità e liquidità del book; (iv) reputazione e solidità; e (v) capacità di integrazione tecnica e reporting, comprese API avanzate e proof of reserves settimanali.

Per ridurre l'esposizione su questi prestatori di servizi in cripto-attività, il team finance supervisiona manualmente le operazioni, mentre le transazioni critiche sono soggette a verifica manuale da parte del team di compliance.

Per quanto riguarda la gestione dei rischi specifici, Conio affronta il rischio di controparte legato a prestatori di servizi in cripto-attività e terze parti attraverso una due diligence iniziale e continua su Kraken e Coinbase, valutandone solvibilità finanziaria, conformità a normative come MiCA e GDPR, report di sicurezza e audit esterni, oltre a stabilire limiti di esposizione massima per ciascuna terza parte.

Sul fronte del rischio informatico, l'azienda conduce penetration test semestrali sui propri sistemi interni e sulle API di integrazione con terze parti, monitorando le transazioni 24/7 con sistemi di rilevamento anomalie, come trasferimenti che superano soglie predefinite. Il rischio operativo è mitigato tramite la segregazione dei compiti: il team di sicurezza e sviluppo non ha accesso alle funzioni di trading, mentre il team finance non può effettuare invii verso wallet esterni.

Quanto ai controlli sull'esternalizzazione a terzi, Conio valuta fornitori come Kraken e Coinbase, classificati come "fornitori critici", attraverso una revisione annuale delle loro licenze e una verifica semestrale delle coperture assicurative e delle riserve. Il monitoraggio attivo è supportato da una dashboard in tempo reale che mostra i saldi allocati su ogni piattaforma, lo stato operativo dei prestatori di servizi in cripto-attività (ad esempio, sospensioni di prelievo) e alert automatici per variazioni anomale delle riserve.

Infine, nel modello Multi Party Computation di Conio, la Terza Chiave viene mantenuta offline dai partner (Banca Generali, Hype) o da un notaio o terzo fornitore per Conio Direct. Il ruolo di queste terze parti è di

mantenere la chiave con finalità di backup o recovery; per Conio sono fornitori di servizi ICT selezionati e monitorati secondo le regole dettate dalla policy di esternalizzazione.

(iv) rendiconto clienti

Conio invierà con cadenza trimestrale, un resoconto dell'operatività del cliente all'indirizzo email registrato.

Il cliente avrà inoltre la facoltà, tramite l'apposita applicazione, di richiedere in qualsiasi momento l'invio dei resoconti già trasmessi oppure di generare un estratto conto per un intervallo temporale specifico, indicando mese/anno di inizio e fine.

Conio, inoltre, fornisce quanto prima ai clienti qualsiasi informazione rilevante sulle operazioni relative alle cripto-attività che richiede una risposta da parte del cliente.

(II) Documenti interni collegati

La presente Policy è integrata dalla **Digital Asset Custody Risk Management Policy - IS40.2** (Cfr. Allegato 33) che ha lo scopo di presentare una tassonomia delle tecnologie e dei rischi ad esse associate, analizzando incidenti reali e dettagliando le contromisure necessarie e adottate da Conio per minimizzare i potenziali impatti. Di tale politica si riporta di seguito una sintesi.

Policy statement

La metodologia utilizzata da Conio per analizzare i rischi di custodia si base su studi e analisi di incidenti del settore. Una lista di incidenti aggiornata, non esaustiva, è proposta da HedgeWithCrypto.

(i) classificazione rischi di custodia

(I) ***wallet risks***

Il wallet è la tecnologia principale per la detenzione di criptovalute ed è lo strumento necessario per firmare crittograficamente le transazioni sulla blockchain. La sicurezza di un wallet dipende da molteplici fattori, in primo luogo dalla gestione delle chiavi private, compresa la loro generazione e conservazione.

- ***rischi tipi di chiave***

Le chiavi possono essere suddivise nelle seguenti categorie:

- hot key, chiavi memorizzate su un dispositivo connesso a una rete, come software desktop/server o un'app mobile. Sono utili per automatizzare i processi di firma, ma comportano rischi maggiori. Se il dispositivo online viene compromesso, un aggressore potrebbe estrarre la chiave privata, caricarla in un altro wallet e utilizzarla per manipolare i fondi all'insaputa del vero proprietario. I metodi di infezione più comuni per i dispositivi online sono: (i) malware [CR1]; (ii) web page watering hole [CR2]; (iii) software dannosi e app mobile [CR3]. Per tutti i wallet che offrono il backup su cloud delle seed phrase, anche questo spazio di archiviazione cloud deve essere considerato come un perimetro da proteggere al fine di prevenire il furto del mnemonico [CR4].
- warm key, chiavi anch'esse memorizzate su dispositivi connessi a una rete, ma sono crittografate e archiviate con una password e/o dati biometrici. In caso di compromissione del dispositivo, l'aggressore dovrebbe trovare una soluzione per decifrare la chiave, ad esempio con un keylogger

[CR5] sul dispositivo compromesso per intercettare la password di decifratura inserita dagli utenti o sfruttare una catena di vulnerabilità [CR6].

- cold key, chiavi memorizzate su dispositivi hardware dedicati, sempre scollegati dalla rete. Il processo di firma avviene internamente al dispositivo, quindi la chiave privata non lascia mai il dispositivo. Tuttavia, se un aggressore entrasse in possesso fisico dell'hardware wallet, potrebbe comprometterlo sfruttando vulnerabilità nel dispositivo stesso [CR7]. A titolo esemplificativo e non esaustivo di attacchi comuni include: side channel attack, voltage glitch attack, Key Negotiation of Bluetooth (KNOB) attack.

Un attacco che può essere applicato a qualsiasi tipo di chiave (hot, warm, cold) è il seedphrashing [CR8] che prevede la creazione e distribuzione di cloni di applicazioni dannose per indurre gli utenti a inserire la propria seed phrase, poi rubata. Un altro è il Clipboard Hijacker [CR9], che prende di mira un dispositivo compromesso in cui il malware altera gli appunti contenenti gli indirizzi di destinazione per l'invio di fondi crittografici, sostituendo il contenuto con un indirizzo controllato da un aggressore.

- **rischi chiavi private e PRNG deboli**

Un rischio che potenzialmente influisce su qualsiasi tipo di chiave è l'insufficiente randomizzazione e la bassa entropia durante la creazione di una chiave privata [CR10]. Le chiavi private vengono generate da un generatore di numeri pseudo-casuali (PRNG), da cui derivano la chiave pubblica e l'indirizzo blockchain; tutte le tecnologie hanno in comune il passaggio iniziale di creazione della chiave privata da un numero (pseudo) casuale. Ciò implica che una generazione di numeri casuali debole durante la creazione di una coppia di chiavi pubblica/privata rende vulnerabile il wallet. Un generatore di numeri pseudo-casuali (PRNG) deve avere il valore di entropia più alto possibile per evitare il determinismo o la prevedibilità dei numeri generati. A titolo esemplificativo e non esaustivo le vulnerabilità relative ai PRNG sono: (i) *Use of Insufficiently Random Values*; (ii) *Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)*; (iii) *Insufficient Entropy*; (iv) *Incorrect Usage of Seeds in Pseudo-Random Number Generator (PRNG)*; (v) *Predictable Seed in Pseudo-Random Number Generator (PRNG)*;

È importante notare che alcune blockchain sono più vulnerabili ai PRNG deboli rispetto ad altre perché non applicano correttamente funzioni hash a valle dopo la generazione di numeri casuali, il che può mitigare i problemi di bassa entropia.

- ***rischi schemi di firma***

Un wallet è caratterizzato da uno schema di firma che può essere: (i) *singlesig*; (ii) *multisig*; (iii) *multiParty Computation* (MPC).

Lo schema *singlesig* si basa su una singola chiave privata associata a un wallet per la firma delle transazioni. Lo schema Multisig coinvolge più chiavi private che contribuiscono alla firma di una transazione; ci sono due numeri, N e M, dove $M < N$, e dove N rappresenta il numero totale di chiavi disponibili nello schema, mentre M rappresenta il quorum, cioè il numero di chiavi necessarie per firmare una transazione. Lo schema di wallet multisig più comune è 2-di-3, dove ci sono un totale di 3 chiavi private e 2 sono necessarie per approvare una transazione. È possibile definire il rischio di un wallet non tollerante ai guasti [CR11] associato a tutti i wallet *singlesig* che non consentono il recupero dei fondi in caso di perdita di chiavi. Allo

stesso modo, è possibile definire il rischio di compromesso singolo [CR12], che consentirebbe a un aggressore di spostare liberamente i fondi in caso di furto di una singola chiave (come analizzato in precedenza con gli attacchi di collisione o altre tecniche di furto di chiavi).

Un altro approccio è l'MPC (Multi-Party Computation). In questo schema, il wallet è gestito da una singola chiave privata che è divisa in N parti (shard). Ciò consente la tolleranza al rischio di perdita di chiavi [CR11] (nello specifico, alla perdita di uno shard di chiave). Tuttavia, non è tollerante al rischio di compromesso [CR12] perché, con una sola chiave privata sulla blockchain, è potenzialmente vulnerabile agli attacchi di collisione. Inoltre, l'MPC introduce ulteriori superfici di vulnerabilità a causa dei protocolli MPC [CR13] stessi che presentano alcune vulnerabilità quali: (i) *Forget-And-Forgive Attack*; (ii) *Lather, Rinse, Repeat Attack*; (iii) *Golden Shoe Attack*; (iv) *Alpha-Rays Attack*.

- **rischi legati alla struttura wallet e al possesso delle chiavi**

Un aspetto fondamentale della sicurezza degli asset crittografici deriva dalla struttura dei wallet e dal possesso delle chiavi private. I wallet non-custodial dipendono dal tipo di archiviazione (hot, warm o cold). I wallet custodial possono offrire una struttura a tre livelli per ciascun account; tuttavia, l'utente non può verificarne le pratiche di sicurezza impiegate dal custode sui singoli livelli, introducendo un rischio di fiducia associato alla gestione delle chiavi archiviate, potenzialmente suscettibili di furto, compromissione e minacce interne [CR14]. Inoltre, i custodi potrebbero avere wallet omnibus e quindi ottenere l'accesso a un wallet consentirebbe ad un aggressore di rubare gli asset crittografici di più utenti [CR15].

(II) ***rischi infrastruttura***

L'infrastruttura IT è un elemento cruciale nella gestione degli asset crittografici. Con self-custody, il rischio è limitato alla rete dell'utente [CR16]. Con soluzioni custodial e ibride, il rischio dipende anche dalla società delegata.

- **rischi esterni:** attacchi al perimetro di un'azienda e includono applicazioni web esposte, API, server VPN, servizi cloud. È essenziale un approccio di sicurezza per il perimetro esterno basato su più livelli di protezione orizzontali e verticali.
- **rischi interni:** attacchi interni di un'azienda e comprendono tutti i servizi interni che non sono esposti (sistemi di back-office, i database, tutti gli endpoint del server e le postazioni di lavoro dei dipendenti); tutti i rischi a cui un'azienda è esposta dalla sua rete interna, sia essa on-premise o basata su cloud (VPC); attacchi condotti tramite phishing mirato ai dipendenti o minacce interne.
- **rischi supply chain:** gli attacchi APT sfruttano vulnerabilità esterne e interne per ottenere accesso, controllo e persistenza all'interno dell'infrastruttura. Questo approccio di attacco è noto come attacco alla catena di approvvigionamento. Rischi comuni: scarsa gestione ambienti [CR17], vulnerabilità servizi esposti [CR18], vulnerabilità servizi interni [CR19], mancanza di utilizzo di WAF/IDS/EDR/XDR [CR20–24], crittografia insufficiente [CR25], sicurezza inadeguata ella generazione e archiviazione dei segreti [CR26], credenziali deboli e mancanza autenticazione a più fattori MFA [CR27], formazione inadeguata [CR28], sistemi di monitoraggio inadeguati [CR29], access control list (ACL) e policy di minimo privilegio inadeguato [CR–30].

(III) ***rischi codice sporgente***

Per la sicurezza di un sistema di custodia è importante la qualità del codice prodotto. Qualsiasi software che contenga bug, errori o vulnerabilità può essere suscettibile di sfruttamento, compromettendo potenzialmente il sistema di custodia. Nel caso dello sviluppo su tecnologia blockchain, la superficie di attacco è più ampia in quanto coinvolge sia software generico che smart contract che operano sulla blockchain.

- ***sicurezza del software***

Per garantire la qualità del software prodotto, è necessario sviluppare una pipeline Secure Software Development Life Cycle (SSDLC). Nel contesto di DevSecOps, gli strumenti utili per garantire una pipeline sicura includono strumenti di Software Composition Analysis (SCA) per l'analisi delle dipendenze, Static Application Security Testing (SAST) per l'analisi del codice e Image Scanning per l'analisi delle immagini software. Ciascuno di questi componenti è cruciale per ridurre al minimo i rischi di vulnerabilità nel software di custodia dell'azienda **[CR31]**.

- ***sicurezza smart contract***

Un rischio tipico di un sistema di custodia nel regno degli smart contract è legato alla gestione dei wallet Ethereum. In particolare, i wallet multisig di Ethereum, essendo sviluppati tramite smart contract, sono potenzialmente esposti a bug e vulnerabilità **[CR32]** che possono comprometterne il corretto funzionamento. L'unica soluzione nota per mitigare questo potenziale rischio è lo sviluppo sicuro di software utilizzando gli strumenti attualmente disponibili sul mercato come Almanax ALMX-1 insieme a audit condotti da società specializzate come Certik.

(IV) ***rischi territoriali***

Un rischio significativo nella custodia di asset digitali è rappresentato dal blocco dei conti crittografici e dall'impossibilità di accedere ai fondi a causa di imposizioni legali territoriali [CR33]. Le restrizioni legali territoriali possono portare al blocco dell'accesso ai conti crittografici e all'impossibilità di disporre dei fondi dei clienti, creando un rischio finanziario significativo per gli utenti interessati. È importante che un custode si trovi all'interno della giurisdizione del territorio locale per evitare rischi di dipendenza finanziaria da altri paesi che potrebbero potenzialmente bloccare servizi critici durante le tensioni geopolitiche; l'intera infrastruttura e le tecnologie di terze parti utilizzate da una società di custodia dovrebbero trovarsi all'interno del territorio locale. Delegare la gestione dei nodi blockchain a una società esterna può comportare rischi di indisponibilità nel caso in cui quest'ultima scarti le transazioni inviate dal custode [CR34].

(ii) ***gestione dei rischi di custodia***

Per tutte le aziende che operano come fornitori di custodia o wallet, è importante seguire regole specifiche per evitare violazioni e mitigare i rischi. Una buona postura di sicurezza non è sufficiente quando si tratta di asset crittografici, poiché la custodia richiede ulteriori best practice (sia tecnologiche che procedurali) che

non si applicano in altri settori. Nella gestione dei rischi di custodia, Conio affronta le minacce indicate con controlli e contromisure adeguate.

- **CR1: compromissione della chiave privata a caldo tramite malware;**
  Contromisure: usare più chiavi e **usare chiavi cold**

la minaccia viene mitigata grazie all'uso di più chiavi e di chiavi cold. Infatti, il portafoglio multisig 2-di-3 di Conio fa sì che una singola chiave non basti a compromettere i fondi. Le chiavi lato client sono memorizzate su HSM he rende i comuni malware incapaci di accedervi anche in caso di infezione del dispositivo se non è rootato. Anche nel caso di dispositivi rooted, Conio dispone di una tecnologia in grado di rilevarlo e di bloccare il wallet. La chiave di Conio è crittografata nel cloud di Conio con una crittografia forte e una rotazione delle chiavi su un servizio cloud gestito e tempestivamente patchato che non è accessibile da Internet; quindi, è molto improbabile che possa essere compromessa. La chiave di recupero (chiave 3) è fredda, conservata suddivisa in N shard su un hardware dedicato senza connettività internet, quindi può essere a rischio solo nel caso in cui un attaccante possa accedere fisicamente a un quorum di shard di chiavi. Dal momento che gli shard delle chiavi sono delegati a diverse parti, è improbabile che costituiscano un rischio se sono gestiti correttamente, come raccomandato da Conio.

- **CR2 (compromissione della chiave privata hot tramite watering hole)**
  Contromisure: usare più chiavi

la minaccia riguarda potenzialmente solo la chiave 1 del cliente. Tuttavia, la sua memorizzazione su un HSM crittografato con segnali biometrici rende inefficaci gli attacchi CDN. Le pagine "watering hole" che cercano di infettare il browser possono avere successo solo su dispositivi rooted. Tuttavia, la tecnologia utilizzata da Conio per rilevare i dispositivi rooted potrebbe bloccare il portafoglio interessato, impedendo a Conio di controfirmare le transazioni.

- **CR3 (compromissione della chiave privata hot tramite app malevola)**
  Contromisure: usare più chiavi e usare chiavi cold

l'unica chiave a rischio per CR3 è la chiave 1 (chiave utente). Anche se non si tratta di una vera e propria vulnerabilità del sistema, Conio sta implementando una tecnologia per identificare un potenziale dispositivo falso/emulato con un punteggio di rischio che, se superiore a una soglia, fa scattare un allarme e mette l'utente sotto forte monitoraggio e potenzialmente blocca tale portafoglio.

- **CR4 (compromissione della chiave privata hot dovuta a cloud backup)**
  Contromisure: non fare backup di chiavi hot in cloud e usare più chiavi

Conio non esegue il backup né della chiave 1 né della chiave 3 nel cloud. La sua natura multisig mantiene il portafoglio recuperabile anche in caso di perdita della chiave; quindi, non necessita di backup della chiave.

- **CR5 e CR6 (compromissione della chiave privata warm tramite keylogger e privilege escalation)**
  Contromisure: usare multisig con più parti coinvolte; controllo del dispositivo per abilitare la firma; con la seconda chiave del custode; rafforzare firma utente con MFA; whitelist degli indirizzi per il prelievo

Conio applica la chiave utente warm (chiave 1) con un MFA. La natura multisig del portafoglio rende Conio in grado di bloccare un portafoglio in caso di attività sospette. Inoltre, Conio può utilizzare una policy per inserire nella whitelist indirizzi specifici per il prelievo. Ogni utente ha accesso alla funzionalità di invio di una transazione attraverso un suo personale AddressBook, in cui deve registrare preventivamente l'indirizzo di destinazione e una soglia massima dell'importo di invio; in questo modo Conio è in grado di assolvere vari

compiti: (i) monitorare gli indirizzi registrati dagli utenti per verifiche di sicurezza preventive e (ii) guidare l'utente a fornire informazioni necessarie ai fini di gestione dei flussi di Travel Rule. L'inserimento di un indirizzo in whitelist (realizzata attraverso l'AddressBook) è condizione necessaria (ma non sufficiente) per permettere l'invio dei fondi all'esterno dell'ecosistema di Conio: non è possibile inviare a indirizzi non registrati ma al contempo laddove l'utente inserisca un indirizzo in seguito identificato come sospetto, Conio può riservarsi il diritto di impedire l'invio bloccando l'utilizzo della seconda chiave per quella transazione. L'utente può chiedere l'utilizzo solo tramite supporto clienti. L'interfaccia sarà prevista con il rilascio della versione dell'app contenente il flusso di travel rule. Pertanto, anche in caso di compromissione delle chiavi utente attraverso l'escalation dei privilegi, Conio può monitorare e bloccare l'attività del portafoglio.

- **CR7 (compromissione della chiave privata cold dovuta a vulnerabilità hardware wallet)**
  Contromisure: usare più chiavi

La natura multisig del portafoglio Conio gli consente di tollerare il fallimento di una singola chiave. Per quanto riguarda i wallet cold utilizzati, essi non conservano la chiave, ma solo un frammento; anche in caso di hardware compromesso, l'attaccante non sarebbe in grado di estrarre l'intera chiave.

- **CR8 (compromissione della chiave privata tramite seedphrase phishing)**
  Contromisure: usare più chiavi

La natura multisig del portafoglio protegge dal fallimento di una singola chiave. Se si utilizza l'infrastruttura Conio, l'aggressore dovrebbe invece autenticare un nuovo dispositivo con MFA e KYC.

- **CR9 (invio a indrizzo fake tramite clipboard hijacker)**
  Contromisure: usare più chiavi e whitelist degli indirizzi per il prelievo

Conio non può proteggere completamente dai clipboard hijacker, ma il suo regtech e il whitelisting dei prelievi possono bloccare potenziali prelievi indesiderati verso indirizzi sbagliati.

- **CR10 (collisione di chiavi dovute a PRNG deboli)**
  Contromisure: usare più chiavi; generare le chiavi in ambienti segregati; generale le chiavi con più tecnologie.

Conio utilizza chiavi multiple generate con tecnologie diverse su parti completamente separate. Inoltre, Conio monitora continuamente il proprio codice attraverso gli strumenti SAST e SCA per verificare che le migliori pratiche sulla generazione di numeri casuali e sulla crittografia siano sempre garantite.

- **CR11 (perdita della chiave privata - singlesig)**
  Contromisure: usare più chiavi

Conio è tollerante ai guasti grazie al portafoglio multisig con chiavi multiple assegnate a parti indipendenti

- **CR12 (chiave privata compromessa – singlesig/MPC)**
  Contromisure: usare più chiavi; usare multisig invece dell'MPC se possible
- **CR13 (vulnerabilità algoritmo MPC)**
  Contromisure: usare il multisig invece dell'MPC se possibile; limitare l'MPC per divenire per divenire una chiave di un multisig in più shard

Conio può tollerare la compromissione di 1 chiave privata. L'utilizzo di MPC esclusivamente sulla terza chiave per la suddivisione in frammenti rende Conio resistente anche a potenziali vulnerabilità dell'algoritmo MPC.

- **CR14** (gestione delle chiavi private di un custode inadeguato unito a insider threat)
  Contromisure: usare più chiavi; usare il multisig invece dell'MPC se possibile; dividere la recovery

key con MPC; tenere le recovery keys offline su hardware dedicato; assegnare parti della recovery key a parti indipendenti; adottare segregazione dei compiti e politiche di least minimum privilege per la gestione delle chiavi del custode; utilizzare schemi di derivazione delle chiavi del portafoglio deterministico gerarchico quando possibile (come BIP-39); aggiungere ulteriori livelli di hashing come PBKDF2 per le blockchain non compatibili con BIP-39; generare nuove chiavi per ogni transazione per evitare il riutilizzo degli indirizzi.

- **CR15 (crypto asset detenuti su omnibus)**
  Contromisure: non usare omnibus wallet per mantenere asset di diversi utenti; segregare interamente i portafogli degli utenti, ossia non utilizzare la stessa chiave di terze parti per diversi utenti
- **CR16 (rete utente compromessa)**
  Contromisure: assumere un modello Zero Trust per tollerare reti malevole; usare cifratura in-transit per le API; cifrare i contenuti sia user-side che server-side

Conio adotta un modello di fiducia zero per tollerare reti dannose/compromesse. Tutte le comunicazioni in transito sono crittografate con i più recenti standard disponibili. Tutti i dati at-rest sono archiviati in modo cifrato con chiavi sottoposte a rotation e crittografia quantum-resistant.

- **CR17 (configurazione infrastruttura errata e sicurezza degli endpoint – on-premise o cloud)**
  Contromisure: rafforzare clod security con CSPM; assicurare compliance degli endpoint con i CIS Benchmark; adottare least minimum privilege policy; adottare segregation of duties sia per il personale che per i server; monitorare le attività con un SIEM
- **CR18 (vulnerabilità servizio esposto VPN,API,etc.)**
  Contromisura: condurre vulnerability assessment; assicurare time sensitive patching; rafforzare la sicurezza dell'infrastruttura con un approccio a layer; adottare EDR/XDR per fermare gli attacchi.

Tutti i servizi esposti, come i server VPN e le API, sono monitorati e protetti a più livelli. La valutazione delle vulnerabilità viene condotta in runtime attraverso strumenti automatici e periodicamente manualmente. I servizi sono gestiti in-the-cloud per garantire una patch tempestiva. I servizi non gestiti vengono patchati manualmente su base giornaliera/settimanale in base alla loro sensibilità. Tutti gli endpoint sono inoltre protetti da sonde EDR/XDR e IDS per rilevare e bloccare gli attacchi basati su malware, fileless e 0-day. Le regole XDR consentono il contenimento della rete in caso di compromissione. Le VPN sono protette da certificati criptati protetti da password e 2FA con un provider esterno. I server VPN sono inoltre dotati di port-knocking per essere oscurati da Internet ed essere visibili solo ai client benigni che conoscono la giusta sequenza magica di bussaggio.

- **CR19 (vulnerabilità interna, movimenti laterali e privilege escalation nella rete aziendale)**
- **Contromisure**: condurre vulnerability assessment; assicurare time sensitive patching; rafforzare la sicurezza dell'infrastruttura con un approccio a layer; adottare EDR/XDR per fermare gli attacchi; segregare le reti adeguatamente; rafforzare l'autenticazione dei servizi interni con MFA

I servizi interni sono protetti con una sicurezza EDR/XDR e sonde IDS. Le valutazioni delle vulnerabilità e le patch sono condotte manualmente, periodicamente e automaticamente per i servizi gestiti. Tutte le reti sono adeguatamente segregate per gestire ambienti diversi, così come le applicazioni sono segregate verticalmente per diversi livelli di servizio. L'autenticazione degli utenti avviene tramite SSO e/o con

password e MFA. Ogni utente ha una specifica classe di autorizzazione (ACL) per accedere solo ai servizi realmente necessari per il suo lavoro, con il minimo privilegio.

- **CR20 (mancanza di protezione alle API)**
  Contromisure: usare WAF/security runtime per proteggere le web app e le API

Conio protegge le API attraverso un WAF. Tutto il traffico verso le API viene inoltre filtrato e fatto passare attraverso un gateway API, un Cloudfront e un bilanciatore di carico. Tutte le protezioni insieme funzionano per bloccare gli attacchi OWASP Top 10, botnet e DDoS.

- **CR21** (**misconfiguration e mancata protezione dei container e delle immagini)**
  Contromisure: scansionare le immagini dei container; usare pipeline DevSecOps per ridurre vulnerabilità nel codice sorgente

Le immagini distribuite sul repository di immagini vengono costantemente valutate per rilevare le vulnerabilità a livello di sistema operativo e di applicazione. Un modulo di runtime viene distribuito come sonda in esecuzione sugli endpoint che eseguono il container per monitorare le attività del container e bloccare/rimediare a potenziali situazioni indesiderate.

- **CR22-24 (mancanza di protezione endpoint, di sistemi di rilevamento intrusione di regole di risposta tempestive)**
  Contromisure: installare sonde EDR probe su tutti gli endpoint (workstation e server); creare policy per il containment di endpoint infetti; installare un IDS per rilevare e fermare specifici attacchi (es: brute force); creare automazioni per rispondere tempestivamente a breach con regole XDR/SOAR; contaniment di endpoint infetti per ridurre la diffusione dell'infezione

Tutti gli endpoint (server e workstation) sono protetti da EPP. La sonda EDR è installata per monitorare e rilevare automaticamente gli attacchi. XDR è configurato per contenere automaticamente la rete di endpoint non critici potenzialmente infetti. Gli endpoint critici sono gestiti con una politica più conservativa sia da un team esterno di Threat Intelligence attivato automaticamente dall'EDR sia con il SOC interno. L'IDS è configurato per bloccare gli attacchi noti, come il brute forcing, e per gestire l'Indicator of Compromise (IoC) attraverso un SOC interno per inserire tali indicatori in una blacklist. Nel corso del tempo le regole dell'IDS vengono aggiornate con le nuove tendenze di attacco. Il SOC e l'operazione di sicurezza sono orchestrati attraverso un SOAR.

- **CR25 (mancanza o debole cifratura atres/in-transit)**
  Contromisure: cifrare dati in-transit per evitare MITM attacks e data leak; cifrare i DB at-rest per evitare data breach e data leak

Tutti i dati vengono archiviati e inviati in modo criptato, imponendo la crittografia a riposo e in transito a tutti i carichi di lavoro e ai database. Le chiavi di crittografia sono gestite attraverso il KMS del provider del cloud, al fine di ruotarle e ridurre al minimo il rischio di compromissione delle chiavi.

- **CR26-CR27 (gestione errata di password e segreti; credenziali deboli e mancanza di MFA)**
  Contromisure: adottare una password policy forte; rafforzare l'autenticazione con MFA; proteggere i secrets come API KEY; adottare segregation of duties; adottare politiche di least minimum privilege; adottare una password policy forte; rafforzare l'autenticazione con MFA la gestione delle credenziali è supportata da password policy forti, MFA e segregazione dei segreti.
- **CR28 (mancanza o debole consapevolezza di minacce cyber nel personale) ù**
  Contromisure: condurre corsi di cyber awareness periodici al personale; condurre campagne di

phishing interno per valutare la consapevolezza del personale; definire policy per evitare phishing

Tutto il personale viene formato annualmente con un corso di cyber awareness; periodicamente viene condotta un'immersione dedicata al phishing; a tutti gli utenti viene fornita una sandbox VM isolata da internet che deve aprire gli allegati ricevuti per proteggere la macchina da potenziali infezioni.

- **CR29 (mancanza di monitoraggio di** insider threat**)**
  Contromisure: monitorare tutte le attività del personale; condurre l'audit e la rendicontazione delle attività del personale; proteggere i dati aziendali con le tecnologie DLP; bloccare i dispositivi USB sconosciuti e bloccare la porta USB dei dispositivi del personale
- **CR30** (best practice deboli su ACL e least minimum privilege)
  Contromisure: rispettare gli standard di sicurezza (ISO27001, CIS, SOC2); adottare la segregazione dei compiti; adottare politiche di minimo privilegio

Tutti gli endpoint, le workstation e i server presentano sonde che li rendono adeguatamente conformi agli standard ISO27001, CIS e SOC2. Le procedure in vigore seguono le migliori pratiche di tali standard

- **CR31 (le vulnerabilità software)**
  Contromisure: pipeline DevSecOps con SCA, con SAST, con image scanning; condurre periodicamente test di penetrazione
- **CR32 (vulnerabilità smart contract)**
  Contromisure: preferire il multisig nativo allo smart contract quando è possibile; automatizzare scansione con software SAST; condurre l'audit al contratto smart multisig

La Società ha una procedura che privilegia le funzionalità native della blockchain piuttosto che sviluppare smart contract se non strettamente necessari. L'azienda si concentra costantemente sulle nuove tendenze in materia di sicurezza e vulnerabilità per avere una chiara comprensione di come progettare e non progettare uno smart contract. Nel caso di contratti intelligenti sensibili, è necessario un audit da parte di un'azienda esterna dopo lo sviluppo.

- **CR33 (rischi di territorialità)**
  Contromisure: il custode che opera in una regione dovrebbe essere locale

Conio opera in Italia, non sussiste il rischio.

- **CR34 (rischi di terze parti)**
  Contromisure: il custode dovrebbe gestire i propri nodi blockchain o delegare le aziende locali

Conio evita di delegare a terzi la gestione dell'infrastruttura blockchain. Conio ha il suo nodo blockchain, il suo software wallet, la sua gestione delle chiavi e tutti gli indicizzatori per monitorare lo stato della blockchain.

(iii) gestione scenari di rischio

I rischi analizzati in questo documento possono essere classificati in 2 categorie principali, rispettivamente in:

1. Furto di digital asset: rappresenta lo scenario più critico di compromissione, poiché può compromettere completamente la Triade CIA non solo per dati e servizi, ma anche per il valore patrimoniale dei digital asset trafugati. Rientrano in questa categoria tutti i rischi relativi a: (i) compromissione di chiavi private; (ii) malfunzionamenti software di invio; (iii) *insider threat*.

Impatto IT: CIA
Impatto Economico: Alto
Conio affronta questi rischi, ove possibile, con un approccio security-by-design per implementare soluzioni di risk avoidance. Laddove non esista un avoidance, implementa misure di risk mitigation.

- **Conio Wallet e Schema di Firma - Gestione Rischio:** RISK AVOIDANCE

  Il wallet di Conio è un multisig 2-di-3, pertanto la *blockchain* per approvare una transazione necessita di 2 firme distinte generate da 2 chiavi private differenti su 3, così la compromissione di una sola chiave non basta. Ogni cliente ha un wallet dedicato con un set di chiavi distinte, non si usano omnibus wallet.

- **Gestione Chiavi - Gestione Rischio:** RISK AVOIDANCE

  Le 3 chiavi sono generate e custodite da 3 parti indipendenti, mantenute in ambienti segregati per evitare compromissioni multiple. Le chiavi non vengono mai ricongiunte e le firme vengono effettuate indipendentemente dalle parti con le proprie chiavi private e le transazioni viaggiano solo firmate. Le chiavi quindi non lasciano mai i device che eseguono le operazioni di firma delle transazioni.

- **Generazione Chiavi** - **Gestione Rischio:** RISK MITIGATION

  Le chiavi sono generate con tecnologie diverse per ciascuna chiave in modo che una potenziale vulnerabilità di una libreria PRNG usata per la generazione dei numeri random causi un rischio solo a una delle 3 chiavi generata con tale libreria. Tutte le librerie PRNG usate sono note e consolidate e Conio si assicura nella *pipeline* Jenkins di sviluppo del codice DevSecOps che queste siano sempre aggiornate e sicure tramite image scanning dei container combinato con tool SCA. Ulteriori controlli sulla loro corretta programmazione sono condotte tramite il SAST Sonarqube e regolari penetration testing condotti da società esterne qualificate con cadenza annuale e vendor rotation.

- **Compromissione Chiave 1 (Utente)** - **Gestione Rischio:** RISK ACCEPTANCE/AVOIDANCE

  La chiave 1 dell'utente può essere a scelta (in base al case study, B2C, B2B2C, B2B) *hot* (*risk acceptance*) o *cold* (*risk avoidance*) a seconda del livello di usabilità e rischio residuo desiderato.

- **Compromissione Chiave 2 (Conio)** - **Gestione Rischio:** RISK AVOIDANCE + MITIGATION

  La chiave Conio è warm ossia controfirma una transazione solo a determinate condizioni al fine di mitigare i rischi dovuti a transazioni firmate impropriamente mediante la chiave 1. Nello specifico, le tecniche di *risk mitigation* messe in atto da Conio possono spaziare da (i) *device control*, (ii) *address whitelisting* e (iii) *transaction policies*. Tali politiche sono ad oggi gestite manualmente da Conio. La chiave di Conio è custodita in un TEE del Cloud AWS di Conio. L'uso di un TEE fa sì che la chiave non possa essere estratta né da dipendenti Conio, né da un eventuale attaccante avente accesso alla rete. Tutta l'infrastruttura Conio è dispiegata in multiple Virtual Private Cloud (VPC) non accessibili dall'esterno e segregate il cui accesso è ristretto con le politiche di *least minimum privilege* ai soli dipendenti che ne hanno necessità. Gli accessi alle VPC sono possibili solo tramite VPN protette con certificati crittografati con password e con autenticazione a due fattori (2FA) gestita tramite Cisco Duo Security.

  I server VPN sono configurati con firewall che li rendono visibili solo da un set di indirizzi IP statici in whitelist assegnati agli uffici e agli endpoint di Conio. Se emergono problemi con gli IP statici e la configurazione del firewall, un meccanismo emergenziale di port-knocking con port-sequence segreta consente l'aggiunta di un IP al firewall, fungendo da terzo fattore di autenticazione.

Tutta l'infrastruttura Cloud è configurata conformemente alle best practice di Cloud Security per evitare vulnerabilità dovute a misconfiguration. Queste configurazioni sono monitorate in real-time con Cloud Security Posture Management (CSPM) tramite Crowdstrike e Wazuh. Qualora i presidi preventivi non fossero efficaci, Conio ha fornito su tutti i nodi EC2 una sonda EDR Crowdstrike Falcon e una sonda IDS Wazuh, gestite da un SOC interno con incident detection & response reperibile fuori orario lavorativo tramite un sistema di alerting real time. Specifiche policy di detection attivano workflow XDR per il containment delle minacce, isolando compromissioni e bloccando automaticamente diffusioni, privilege escalation e movimenti laterali. Conio utilizza anche il SOC di Threat Intelligence di Crowdstrike Overwatch 24/7 come ulteriore sistema di prevenzione e detection qualora il SOC interno, l'XDR e i workflow non risultassero efficaci.

Tutti i servizi AWS-managed sono gestiti da Amazon, mentre per i non-managed Conio effettua patch management con controlli periodici e secondo feed di threat intelligence relativi alle piattaforme in uso. Tutti gli endpoint sono mantenuti aggiornati e monitorati con Vulnerability Assessment di Wazuh e Crowdstrike in modalità scan-less. I database sono cifrati at-rest e tutte le comunicazioni cifrate in-transit. Le chiavi di cifratura sono sotto key rotation con AWS KMS per evitare che una chiave intercettata sia valida per tempi indefiniti e riusabile da un attaccante. Il software Conio è eseguito in microservizi containerizzati Docker per efficienza e sicurezza: tutti i container sono monitorati dal Docker Scanning di Wazuh. Se necessario, l'escalation dal container all'istanza EC2 può essere bloccata dall'EDR di Crowdstrike.

- **Compromissione Chiave 3 (Recovery - terze parti)** - **Gestione Rischio:** RISK AVOIDANCE + MITIGATION

Questa chiave è sempre cold e divisa in N shard, di cui è necessario con quorum per la firma. Conio usa questa chiave come ulteriore meccanismo di *risk mitigation* per assicurarsi di non controfirmare una transazione firmata dalla chiave 3 se non è stata creata un apposita procedura di *recovery* per cui l'utilizzo di questa chiave è pensata.

2. Perdita digital asset: rappresenta uno scenario critico che può compromettere parzialmente o interamente l'integrità e la disponibilità di dati e servizi, nonché il valore patrimoniale parziale o totale dei digital asset smarriti. Rientrano in questa categoria tutti i rischi relativi a (i) smarrimento chiavi private (danni accidentali, attacco ai database, etc); (ii) insider threat (relativi alle capacità di cancellazione o modifica di dati essenziali).

Impatto IT: IA

Impatto Economico: Alto

Conio gestisce i rischi afferenti a questa categoria con un approccio *security-by-design* al fine di implementare soluzioni di *risk avoidance*. Solo nei casi dove non esistono soluzioni di *risk avoidance*, Conio implementa soluzioni di *risk mitigation*.

- **Smarrimento Chiave 1 (Utente)** - **Gestione Rischio**: RISK ACCEPTANCE / MITIGATION

Il *wallet* Conio consente di recuperare sempre i fondi qualora 2 chiavi qualsiasi su 3 siano disponibili. A seconda della metodologia di chiave 1 scelta dall'utente (*hot* o *cold*) il rischio può essere accettato o mitigato. Nello specifico, in caso di singola chiave 1 *hot*, in caso di smarrimento, si procederà con il sistema di *recovery* di Conio denominato Titan coinvolgendo le terze parti e Conio per la movimentazione dei fondi

su un nuovo portafoglio creato appositamente per l'utente che ha smarrito la chiave. Nel caso di utenza con chiave *cold*, la perdita o il malfunzionamento di un qualsiasi *shard* non comporta necessariamente l'utilizzo di Titan in quanto è possibile usare gli altri *shard* fintanto che esiste un quorum. Qualora lo smarrimento o il malfunzionamento riguardi più dispositivi *hardware* e questo creasse un livello di rischio definito non accettabile, si può procedere con la recovery mediante Titan andando quindi a invalidare i vecchi *shard* e rigenerando un nuovo portafoglio con una nuova cerimonia di creazione dell'intero *set* di chiavi (pertanto anche dell'*hardware* con gli shard della chiave 1).

- **Smarrimento Chiave 2 (Conio)** - **Gestione Rischio**: RISK TRANSFER + MITIGATION

La chiave Conio è custodita su TEE Cloud di AWS, Conio affida, la gestione ordinaria ad AWS (risk transfer) per il mantenimento disponibile, consistente e integro combinato con soluzioni di risk mitigation nei casi di potenziali problemi dell'ambiente AWS usato. Il backup e disaster recovery plan di Conio prevede l'esecuzione di backup periodici su availability zone diverse, in datacenter indipendeti e region differenti.

- **Smarrimento Chiave 3 (Recovery - terze parti)** - **Gestione Rischio**: AVOIDANCE + MITIGATION

Il sistema di chiavi *cold* con gli N *shard* evita e mitiga il rischio di smarrimento della chiave 3 e, conseguentemente, l'impossibilità di effettuare recovery nel caso in cui gli utenti perdessero la propria chiave privata e prevede un successive ripristino della chiave. Un singolo *insider* anche in questo caso rappresenta un rischio minimo, in quanto essendo in possesso di un solo *shard* non potrebbe effettuare alcuna operazione.

(iv) analisi e gestione dei rischi residui

Per rischio residuo si intende quella porzione di rischio residua a valle delle contromisure adoperate da Conio.

A. <u>*Rischi residui intrinsechi (ineliminabili):*</u> (i) blackout su larga scala e interruzioni della rete (non sono previste contromisure); (ii) interruzioni delle reti blockchain che, essendo tecnologie distribuite, possono funzionare fintanto che esiste anche un solo nodo. Conio, garantendo di mantenere attivo il proprio nodo, può ridurre tale rischio. Nei casi d'uso di tokenizzazione può invece offrire il supporto

   di migrazione verso altre chain; (iii) reti *blockchain* byzantine compromesse. Conio tramite le analisi *on-chain* condotte di *routine*, potrebbe segnalare con tempistiche ragionevolmente basse eventuali problemi per suggerire una movimentazione dei fondi su altre *chain* tramite *bridge;* (iv) crittografia ECDSA/EdDSA e funzione di hashing, usata per la generazione dell'indirizzo del *wallet multisig* generato a partire dalle 3 chiavi pubbliche, rotte (invertibili) contestualmente; (v) vulnerabilità 0-day su 2-di-3 generatori PRNG usati da Conio per la generazione delle chiavi private, Conio sta introducendo un sistema di creazione delle chiavi private combinando i PRNG con un generatore quantistico QRNG (in fase di brevetto) per ridurre anche tale rischio residuo (vi) chiavi *cold* inaccessibili dovute a rotture contestuali di hardware, Conio può usare chiavi cold provenienti da lotti differenti.

B. <u>*Rischi residui gestibili da Conio:*</u> (i) sistema di invio fondi rotto o malevolo; (ii) utilizzo errato dei PRNG per la generazione delle chiavi. In tale ipotesi caso Conio si impegna ad adoperare gli strumenti di analisi del codice con un SAST e audit del codice per la funzione relativa agli invii e di creazione delle chiavi

C. *<u>Rischi residui dovuti a collusioni tra 2 di 3 parti:</u>* (i) collusione tra utente e terze parti; (ii) collusione tra Conio e terze parti.