RDAEL Client Assets Safeguarding Policy and Plan

Revolut Digital Assets Europe Ltd
Effective Date: 04 November 2026

Table of Contents

1. Introduction
1.1 Objectives and scope
1.2 Authorisation
1.3 Key definitions
2. Document content
2.1 General requirements
2.2 Separation and segregation of clients assets
2.3 Due Diligence of third parties
2.4 Use of crypto assets of clients
2.5 Creation and safeguarding of cryptographic keys
2.6 Maintenance of assets
2.7 Entitlements of clients
2.8 Information provided to clients
2.9 Procedures in place to return assets to clients
3. Business Model
3.1 Regulated services
3.2 Omnibus Account
3.3 Transactional Activity
3.4 Custody and Payment of Gas Fees
3.5 Reconciliation Procedures
3.6 Client Statements
3.7 Internal Materials
3.8 Policy review

1. Introduction

1.1 Objectives and scope

This Policy is designed to ensure compliance with the following legal and regulatory requirements:

MiCA (EU Regulation 2023/1114), specifically Articles 68 (Organisational Requirements), 70 (Safekeeping of Client Assets), 73 (Outsourcing), and 75 (Custody and Administration of Crypto-Assets);
The primary objectives of the Client Assets Safeguarding Policy and Plan are as follows:

- Safeguarding Client Assets: To ensure the protection and security of crypto assets held on behalf of clients in accordance with applicable regulations and internal controls.
- Risk Mitigation: To outline the business model and associated risks regarding the safeguarding of client assets and the measures in place to mitigate these risks.
- Transparency and Accountability: To enable the Board of RDAEL to document, monitor, and evaluate material changes to business processes, controls, and associated risks impacting the safeguarding of client assets.
- Asset Distribution in Case of Insolvency: To facilitate the prompt distribution of client assets, particularly in the event of RDAEL's insolvency, by making necessary information readily available.
- Third-Party Relationships: To provide an in-depth analysis and breakdown of RDAEL's relationship with third-party exchanges and custodians, ensuring appropriate safeguards for client assets.

RDAEL recognises the critical importance of safeguarding and protecting client assets in its operating model. RDAEL does not process or hold any fiat for or on behalf of its clients. The Client Asset Safeguarding Policy and Plan (the "Policy') seeks to address the below areas:

- To outline RDAEL's business model and related risks in respect of the safeguarding of client assets and the controls in place to mitigate these;
- To demonstrate how RDAEL's systems and controls meet the principles of the client asset regime;
- To enable the Board of RDAEL (the "Board") to document and monitor material changes to RDAEL's business model, changes to controls and processes and any changes regarding the associated risks to safeguarding client assets; and
- To make information readily available to assist in the prompt distribution of client assets, particularly in the event of RDAEL's insolvency.

The Policy is a "living" document which is continuously reassessed and evolves with the business. The Policy documents key judgements regarding the business model, materiality and risk framework in relation to the safeguarding of client assets.
Given the purpose of the Policy, as that is identified above, RDAEL is considered to be in a good position to provide an in-depth analysis and breakdown of the relationship it will have with third party exchanges and custodians in terms of safeguarding and protecting client assets.
RDAEL's operating model in relation to crypto assets is based on operating omnibus wallets with third party exchanges and custodians.

1.2 Authorisation

RDAEL obtained its authorisation and acts as a crypto asset service provider under the EU Regulation 2023/1114 on markets in crypto assets ("MiCA") since 20 October 2025. Under its license, it is authorised to the following services:
1. providing custody and administration of crypto-assets on behalf of clients;

2. operation of a trading platform for crypt-assets;
3. exchange of crypto-assets for funds;
4. exchange of crypto-assets for other crypto-assets;
5. placing of crypto-assets; and
6. providing transfer services for crypto-assets on behalf of clients.

For the purposes of this Policy, 'providing custody and administration of crypto- assets on behalf of clients' means the safekeeping or controlling, on behalf of clients, of crypto-assets or of the means of access to such crypto-assets, where applicable in the form of private cryptographic keys.

The scope of RDAEL's services related to safeguarding (custody) of the crypto assets will include:

- Making settlements of executed transactions;
- Processing certain actions (e.g. changes in response to a fork event);
- Recording and accounting of the crypto assets in the omnibus wallets;
- Providing statements of the crypto asset wallets and other reports to clients and/or to authorities (e.g. the Cyprus Securities and Exchange Commission).

1.3 Key definitions

- Client Assets: Refers to the crypto assets held by RDAEL on behalf of its clients.
- Omnibus Wallet: A type of wallet where the assets of multiple clients are pooled together in one collective account.
- Custody: The safekeeping or control of crypto-assets on behalf of clients.
- Third Party: Refers to any external custodian, exchange, or entity that holds crypto assets on behalf of RDAEL and its clients.
- Due Diligence: The process by which RDAEL evaluates the suitability, reputation, and regulatory compliance of third parties before engaging in agreements involving client asset custody.
- Cold Wallet: A crypto wallet that is not connected to the internet, used for storing crypto assets securely, typically to reduce the risk of cyber-attacks.
- Hot Wallet: A crypto wallet that is connected to the internet, providing immediate access to assets but carrying a higher risk due to its connectivity.
- MiCA: The EU Regulation 2023/1114 on Markets in Crypto Assets, which provides a regulatory framework for the crypto asset market in the EU, including the safeguarding of client assets.
- Insolvency: A scenario in which RDAEL is unable to meet its financial obligations, necessitating the distribution of client assets back to clients.
- Entity-level segregation: The requirement that RDAEL client assets are held in wallets and venues dedicated to RDAEL, not commingled with other group entities, except for strictly controlled, temporary exceptions (e.g., legacy deposits, frozen assets).
- MiCA-licensed venue: A third-party custodian or exchange licensed under MiCA to provide custody and administration of crypto-assets.
- Fireblocks workspace: A dedicated custody environment within Fireblocks, used for holding and managing client assets.

Changes from previous versions

Version No.	**Approval Date**	**Summary of changes from** previous versions
Version 1.0	30 December 2024	Introduction of Policy
Version 2.0	April 2025	Update to incorporate the OTC and OTP trading models
Version 3.0	August 2025	Update to incorporate the new custody arrangements, i.e. the bilateral (as opposed to tripartite) agreements between RDAEL and third party exchanges and the increased control over Fireblocks
Version 4.0	October 2025	Removed paragraphs that caused repetition. Clarified that assets of clients of RDAEL will be held at MiCA compliant exchanges and Fireblocks
Version 5.0	March 2026	Update in relation to segregation of wallets

2. Document content

Safeguarding of clients' crypto assets

2.1 General requirements

RDAEL's safeguarding arrangements are designed to ensure that, at all times, client assets are segregated at the entity level, in line with CySEC's requirements and MiCA Art. 70.
RDAEL shall take adequate measures to protect and safeguard the assets belonging to its clients, including:

- Keep records and accounts in a way that RDAEL is capable, at any time and without delay, to distinguish the assets held for one client from the assets held for any other client and from the assets of RDAEL;
- Maintain records and accounts in a way that ensures their accuracy, and their correspondence to the assets held for the clients, and in a way that such records and accounts can be used as an audit trail;
- Conduct monthly reconciliations between the internal information, on total client balances to those of third parties by whom assets are held;

- Take necessary steps to ensure that assets of the clients, deposited with a third party, are identifiable separately from the assets belonging to RDAEL and to that third party and have the same level of protection as in RDAEL in accordance with this Policy;
- Take relevant organisational measures to minimise the risk of the loss or diminution of the assets belonging to clients, or of rights in connection with those crypto assets, as a result of misuse of the assets, fraud, poor administration, inadequate record-keeping or negligence.

2.2 Separation and segregation of clients assets

RDAEL's safeguarding arrangements are designed to ensure that, at all times, client assets are segregated at the entity level, in line with CySEC's requirements and MiCA Art. 70.
Assets belonging to RDAEL's clients are kept separate from:

- the assets belonging to RDAEL; and
- the assets belonging to clients of other entities within the Revolut group, with certain exceptions described in this Policy.

Assets belonging to RDAEL's clients are held exclusively within RDAEL's dedicated Fireblocks workspaces and MiCA licensed custody venues, ensuring they are strictly segregated from both RDAEL's proprietary assets and the client assets of other Revolut Group entities. The only exceptions to the latter are specific assets frozen for financial crime compliance or legacy positions undergoing phased migration, all of which remain clearly ledgered and protected under RDAEL's safeguarding framework.
RDAEL aims to maintain a 1:1 backing of client liabilities as close as possible within these dedicated environments. Given the inherent latency of blockchain settlements and the volatile nature of crypto trading, there may be short periods during active rebalancing windows during which assets are in transit between entities, resulting in temporary mismatches between the assets held in RDAEL-designated wallets and its corresponding client liabilities; however, RDAEL employs automated "sweeps" to minimise such mismatches and to ensure that no unauthorised or prolonged commingling occurs.
RDAEL shall inform the clients via T&C or otherwise, that RDAEL may hold the assets belonging to a client:

- in an individual user wallet; or
- together with the assets belonging to other client(s) in an omnibus wallet.

Where RDAEL keeps the clients' assets in an omnibus wallet or in a wallet opened in the name of RDAEL, then it shall always keep separate records of the crypto assets belonging to each client.
RDAEL may deposit crypto assets of the clients into one or more of the following wallets: (a) self custody wallets, (b) hot wallets, and (c) cold wallets. This applies to RDAEL's Retail and Business clients opening a crypto account in the Revolut App and/or opening an account in the Revolut X trading platform.
Self Custody wallets
This encompasses the crypto assets RDAEL holds with Fireblocks which is a Multi Party Computation (MPC) wallet, where RDAEL maintains a direct contractual agreement with Fireblocks. Under this setup, RDAEL holds the majority of the components of the private keys.

This solution is largely used to facilitate Remittances, Staking, moving crypto assets between exchanges and cold storage.
Fireblocks is a provider of the relevant IT infrastructure and as such does not need to be licensed under MiCA as it does not provide any services of custody and administration of crypto-assets on behalf of clients.
Hot Wallets
This encompasses the crypto assets RDAEL holds with Fireblocks and third party exchanges. A hot wallet is defined as a wallet that has active internet connectivity and where the legal owner or trustee of the crypto assets (i.e. RDAEL) does not own the private keys. While it is less secure than a cold wallet solution, it allows for immediate access to the crypto assets to facilitate trading orders and therefore hot wallets are used to facilitate buy and sell transactions of RDAEL clients.
For RDAEL to be able to hold clients' crypto assets into hot wallets with third party exchanges, such third party exchanges need to be licensed under MiCA.
Cold Wallets
This encompasses the crypto assets RDAEL holds in cold storage. A cold wallet is defined as a wallet that has no internet connection. Such wallets are utilised for enhanced security as they are offline or air-gapped, making them significantly less prone to cyber attacks due to the lack of a permanent internet connection. In order to leverage these crypto assets and facilitate clients' buy and sell orders, crypto assets on cold wallets first need to be moved to a hot wallet. Given the high-security nature of moving funds from cold custody to hot wallets, RDAEL enforces a strict multi- signature quorum. This requires multiple independent approvals from multiple authorised personnel across Revolut, ensuring that no single individual or admin can unilaterally move funds from cold custody. The majority of client crypto assets are kept on cold wallets.
RDAEL does not at any time hold any client funds (fiat currency).

2.3 Due Diligence of third parties

RDAEL may deposit crypto assets belonging to a client into wallets opened with a third party only if it exercises due skill, prudence and diligence in:

- selection and appointment of such third party;
- periodic review over such third party; and
- periodic review over the arrangements of the holding of the crypto assets.

RDAEL shall evaluate the following criteria when selecting suitable third parties:

- The expertise and reputation of such third party;
- Legal requirements or market practices related to the holding of specific crypto assets that could adversely affect clients' rights; and
- That such third party must be itself licensed under MiCA to provide custody and administration of crypto-assets on behalf of clients.

RDAEL shall perform the verification and evaluation of the third party and record the results in writing and/or electronically every time before entering into an agreement with a third party.
When necessary, RDAEL shall initiate an exhaustive assessment of the impact of the third party and the legal system of its member state of establishment and potential insolvency on the clients' crypto assets.

Third parties where crypto assets belonging to clients will be deposited will be approved by RDAEL's Executive Risk Committee.
Group Third Party Risk Management Policy shall also be applied when depositing crypto assets belonging to the client with a third party.
All third-party custodians and exchanges must be MiCA-licensed for custody. RDAEL's Group Outsourcing and Third-Party Management Policy applies to all such arrangements.
RDAEL systematically monitors and oversees third-party vendors who are governed by direct agreements with RDAEL such as third parties holding the clients' assets. The comprehensive oversight process includes conducting annual attestations, which serve to thoroughly reassess vendor due diligence practices. These attestations are designed to identify any breaches of contract that may have occurred, evaluate whether appropriate exit strategies are in place, and validate the integrity of the data handled by the vendors.
Additionally, the RDAEL outsourcing department carefully detects potential instances of data duplication and conducts a detailed review of service level agreements (SLAs) to ensure compliance and performance standards are met. To effectively capture and measure these critical areas, seven Key Risk Indicators (KRIs) are employed, providing a structured framework for risk assessment and management throughout the vendor oversight process.
Operations shall inform RDAEL risk and compliance units about any noticed deficiencies in the third parties' operation and in performance of their functions related to custody of crypto assets. In case it is found out at any time that the third party does not comply with the requirements of the legislative acts, RDAEL shall take the following actions:

- Initiate the termination of the agreement with the third party;
- Initiate signing of an agreement with another third party pre-identified by RDAEL that complies with the requirements provided for in MiCA;
- Organise signing of the agreement with a third party; and
- Take other actions, which it considers necessary, to maintain the clients' crypto assets and avoid damages and losses.

2.4 Use of crypto assets of clients

RDAEL may not pledge the crypto assets of clients in its own interest or in the interest of a third party. RDAEL may not use crypto-assets belonging to the clients for its own account in any way. To ensure that clients' crypto assets are not used for RDAEL's own account, a number of controls are in place and documented in the Cryptocurrency Risk Management policy. These include key risk indicators, treasury controls and transaction reconciliation process, as detailed below.

- A Key Risk Indicator that monitors and compares the value of crypto asset balances held by clients and the value of balances held across all crypto asset workspaces (e.g. Fireblocks, crypto exchanges and cold custody).
- Treasury controls to prevent bad actors from moving crypto assets to unapproved accounts. All accounts involved in crypto-related transactions require whitelisting involving a maker / checker approval process. The initial movement of funds between accounts requires test transitions and maker / checker approval on these transactions to validate the sending and reconciliation of these test flows.

- Transaction reconciliation process to ensure all transactions are reconciled against the above tested flows. A ‘break’ in transactions will occur if there is a difference in e.g. values, dates of transactions and accounts from which the transactions were sent to and from, between the actual transaction and the intended transaction that Revolut records internally to ensure accuracy of movements.

2.5 Creation and safeguarding of cryptographic keys

Overview
A Fireblocks Vault employs a secure multi-party computation (MPC) based architecture for managing cryptographic keys. Distinct from traditional wallets that rely on a single, potentially vulnerable private key, Fireblocks' MPC protocol fundamentally avoids the creation of a unified, recoverable private key at any point. Instead, transaction signing is achieved through a collaborative process involving multiple independent key shares. This distributed cryptographic approach inherently eliminates the single point of failure characteristic of conventional key management systems.
Creation of Cryptographic Key Shares
The generation of private key shares within the Fireblocks platform leverages hardware random number generators (HRNGs) to ensure a high degree of entropy, meeting stringent randomness requirements for cryptographic security. This process is fully automated, eliminating the risks associated with manual key generation procedures. If the MPC key generation process encounters any failure, the respective key share is not created, ensuring the integrity of the process.
In the MPC framework, each participant securely generates its individual key share. These shares collectively enable the Fireblocks workspace to conduct cryptographic operations without ever reconstructing a complete private key. The key shares remain independent and are never aggregated. For transaction signing, each key share independently computes a partial signature without revealing its underlying secret. These partial signatures are then cryptographically combined to produce a valid transaction signature.
This methodology guarantees that a complete, unified private key for the workspace is never formed or accessible in a single environment. Consequently, the extended private key, representing the collective signing capability, does not exist as a tangible, storable entity. The sole exception to direct online accessibility is the Workspace Key Backup and Recovery mechanism designed for disaster recovery. In this scenario, the individual key shares are securely encrypted and stored within a recovery package on an offline, air-gapped machine protected by hardened access permissions.
Each individual MPC key share is generated within a hardware-isolated component utilizing a NIST SP 800-90A compliant random number generator (Intel RDRAND), thereby significantly mitigating the risk of protocol implementation weaknesses or predictability.
Safeguarding of Cryptographic Key Shares
Fireblocks employs a differentiated approach to safeguarding key shares depending on the signer type:

- **Mobile Signing Devices:** For each mobile signing device, one key share is securely generated and stored on the device itself. Two corresponding key

shares are generated and maintained within two geographically separate and secured Software Guard Extensions (SGX) enclaves hosted on independent infrastructure.

- **API Signers:** For API-based signing, all three necessary key shares are generated and securely stored within three distinct and geographically separate SGX enclaves.

Protection of Key Shares on Mobile Devices:

Key shares stored on mobile devices are protected through multiple layers of security, including secure storage mechanisms provided by the operating system (e.g., iOS Keychain) and robust encryption. Access to these key shares for signing operations requires successful authentication and decryption based on a combination of:

- **Knowledge Factor:** "Something you remember" (PIN code).
- **Biometric Factor:** "Something you are" (Touch ID or Face ID).
- **Possession Factor:** "Something you have" (e.g., YubiKey NFC).

This multi-factor authentication mechanism significantly reduces the risk of unauthorized access and key compromise.

Protection of Key Shares within SGX Enclaves:

Intel SGX provides a hardware-based Trusted Execution Environment (TEE), creating isolated enclaves within the system's memory. These enclaves offer a high level of protection for sensitive code and data, including cryptographic key shares. The memory space and data within an SGX enclave are encrypted and integrity- protected at the hardware level. This design ensures that even if the underlying operating system or hypervisor is compromised by malware or malicious actors, the key shares within the SGX enclave remain inaccessible and protected. This effectively mitigates risks associated with both external attacks and insider threats, including those from rogue administrators.

Key recovery procedures

The first step of the key recovery process is to set up the offline recovery machine. This involves setting up a secure, offline, air-gapped machine through software provided by Fireblocks. This step is deemed complete once we generate the recovery keypair, the public key is shared with Fireblocks who will perform an integrity check on the key and the key is then backed up via a Fireblocks Key Backup

Package. Then a sanity test is performed to ensure steps have been carried out accurately. Under a disaster scenario whereby we need to recover the private key, at the request of the RDAEL CEO, RDAEL employees will be provided access to the offline, air- gapped machine by the InfoSec team to reconstruct the extended private key. This is done via the Offline Recovery Tool, which requires a password from RDAEL colleagues. InfoSec team cannot act unilaterally in this circumstance nor do they have any access to the Fireblocks workspace; this situation of reconstructing the private key is initiated by an RDAEL employee. The only input InfoSec has in this scenario is the provision of the air-gapped machine.

Once the extended private key is generated, this can be used to generate the private key for specific vaults, ensuring there is no impact to client funds.

Additional Security Measures:

In addition to the inherent security of the MPC protocol and the protection of individual key shares, Revolut implements supplementary security controls, including annual security sanity tests and a comprehensive disaster recovery process. This disaster recovery plan is aligned

with Information Security best practices and is subject to their oversight, ensuring the continued security and availability of our crypto assets.

2.6 Maintenance of assets

RDAEL combines third-party hot wallets, and secure offline cold storage in MiCA- compliant custodians. RDAEL's clients assets are held in centralised omnibus accounts/wallets maintained at a partner MiCA compliant crypto exchange or in RDAEL's Fireblocks wallet. Clients's assets in cold storage are not combined with other entities. Thus, RDAEL is balancing liquidity needs with asset security and regulatory compliance achieving also operational and financial efficiencies.

RDAEL maintains a register of positions and is able to determine at any given moment the outstanding balance of its clients' assets. RDAEL maintains a high degree of oversight and control over the custody of its clients' assets to ensure compliance with MiCA requirements.

The register of positions maintains a record of each RDAEL client's balance per token, updated multiple times per hour. This process ensures that, in the event of an insolvency, assets can be accurately and promptly returned to clients. Additionally, the register enables comprehensive oversight of balances by user, currency, and entity.

The register is managed by a dedicated data team and is accessible in a non-PII format to authorized personnel, specifically members of the crypto team, treasury colleagues, and market-making staff.

To ensure continuity, the database supporting this register is monitored for uptime, with alerts configured to notify relevant teams in the event of any downtime.

RDAEL shall at its sole discretion decide whether to support any event that creates or modifies the rights of a client.

2.7 Entitlements of clients

When executing transactions on RDAEL's platforms (Revolut App and Revolut X), users appoint RDAEL as their nominee to hold cryptoassets on their behalf. RDAEL holds legal title to the cryptoassets, while users retain beneficial ownership, granting them full rights to their financial value. Users have control over their cryptoassets through instructions given to Revolut via the relevant app to only sell, transfer, or withdraw, although transactions cannot be executed directly by them.

For staking transactions, users agree via our terms that we or our partners (staking providers) are solely responsible for all staked assets' governance decisions regarding the staking services, and instruct us or our partners to exercise any voting right(s) on their behalf.

Similarly, for scenarios such as airdrops, we do not guarantee that ownership of a token entitles users to participate in such events.

The Terms and Conditions and client summary are updated to reflect the new custody model, entity-level segregation, and MiCA requirements.

2.8 Information provided to clients

RDAEL includes in its Terms and Conditions a clear and concise summary in a non- technical language the key aspects of RDAEL's systems and policies and procedures to comply with its safeguarding obligations.

2.9 Procedures in place to return assets to clients

There are two scenarios in which RDAEL may return crypto assets to a user:

1. **User-Initiated Return of Funds to their Wallet**

In a non-stressed scenario, a user may request to sell their crypto asset for fiat or another currency through the RDAEL's platforms (Revolut App and Revolut X). In such cases, RDAEL will verify that the requested transaction value does not exceed the value of the crypto assets the user intends to sell. Provided this condition is met, and there are no account limits in place, the transaction will proceed. This balance verification process is conducted in near real-time. Alternatively, a user may request the transfer of crypto assets to an external wallet not held by Revolut. For this scenario, a similar balance check will be performed. If the account holds sufficient balances and no restrictions are active, the transaction will be executed as requested.

2. RDAEL-Initiated Return of Funds to a User

RDAEL may initiate the return of funds to a user in certain circumstances. Such requests are initiated by RDAEL. These include, but are not limited to, situations where RDAEL is delisting a specific token, closing a user's account, or complying with an order from a regulatory body to cease support for a particular token.

In such stressed scenarios, RDAEL will endeavor to provide users with advance notice regarding the upcoming liquidation of assets. For example, RDAEL typically aims to give 14 calendar days' notice, allowing users the opportunity to sell the token, convert it into another token, or withdraw it from the platform. Should the user fail to take action by the liquidation date, RDAEL will proceed to liquidate the holdings, converting them to the user's local currency, and will credit this amount to the user's fiat account. In cases where the value of the holdings is less than the smallest denomination of the user's local currency, RDAEL will credit the account with the smallest unit (e.g., EUR 0.01 for users in the EEA where local currency is in Euro).

3. Business Model

The below provides an overview and the plan on how clients' assets safeguarding requirements are to be observed by RDAEL in the course of its operations.

3.1 Regulated services

RDAEL provides crypto services to clients based within the EEA. RDAEL also provides crypto services to clients based in Switzerland on a reverse solicitation basis. The services listed in section 1.2 above are provided to Retail and Business clients opening a crypto account in the Revolut App and/or opening an account in the Revolut X trading platform, which is operated by

RDAEL. Via the Revolut App, RDAEL directly executes trades with customers, by exchanging crypto-assets for funds or other crypto-assets, without routing immediately to an external venue. RDAEL acts as the counterparty to the customer trade and takes full execution risk, determining when and how to hedge open positions. Via Revolut X, RDAEL operates a trading platform allowing its customers to make or take liquidity and trade with each other.

3.2 Omnibus Account

RDAEL maintains a register of positions and is able to determine at any given moment the outstanding balance of its clients' assets. It is important to note that Revolut Ltd also has access to the wallets where RDAEL clients' assets are stored, as part of the operational structure that facilitates the execution of client transactions. However, RDAEL retains control and oversight of its clients' assets. RDAEL has dedicated workspaces for its clients through a direct agreement with Fireblocks. RDAEL exercises positive control over the Transaction Autorization Policy (TAP), which is the transaction signing policy on Fireblocks. No change can take place without the sign off from the owner of the workspaces which is RDAEL's CEO. This means that RDAEL participation is mandatory regarding activities such as the whitelisting of accounts, amending the Transaction Authorization Policy and connecting to new exchange accounts. For any amendments to the TAP, a quorum of at least two approvals is required, meaning no employee is able to act independently or without RDAEL engagement. Quorum can be met by RDAEL employees only.

3.3 Transactional Activity

Clients must first open a bank account with Revolut Bank UAB (RBUAB) or Revolut Bank S.A. (RBSA) depending on where they live, as all activities the client undertakes with RDAEL are funded from the balance of the client's money account with RBUAB or RBSA. The creation of the client money account and the onboarding process are completed using the Revolut App. Once onboarded into the Revolut App, an RBUAB or RBSA client can access RDAEL's crypto services through the
Revolut App by clicking on the Crypto widget. The client can then become an RDAEL client by following the crypto onboarding steps, including accepting new terms and conditions relating to RDAEL's crypto services offering. Once onboarded into the Revolut App, an RBUAB or RBSA client can also set up a separate crypto account on Revolut X via this link. The client can then become an RDAEL client by following the crypto onboarding steps, including accepting new terms and conditions relating to RDAEL's crypto services offering via Revolut X.
Clients must have sufficient funds on their account (Revolut App and/or Revolut X) in order to facilitate a purchase order. Funds can be debited directly from clients' bank account held with RBUAB or RBSA main account in-app.
Clients must have sufficient crypto on their account (Revolut App and/or Revolut X) in order to facilitate a sell order.
Clients can then submit an order (buy or sell) via the Revolut App or Revolut X.

3.4 Custody and Payment of Gas Fees

Custody

As noted in the 'Omnibus Account' subsection, RDAEL holds client funds within omnibus treasury vaults (i.e. Fireblocks) and transfer client funds to wallets in order to manage liquidity and rebalance the wallets as to facilitate its crypto services to the clients.

Payment of Gas Fees

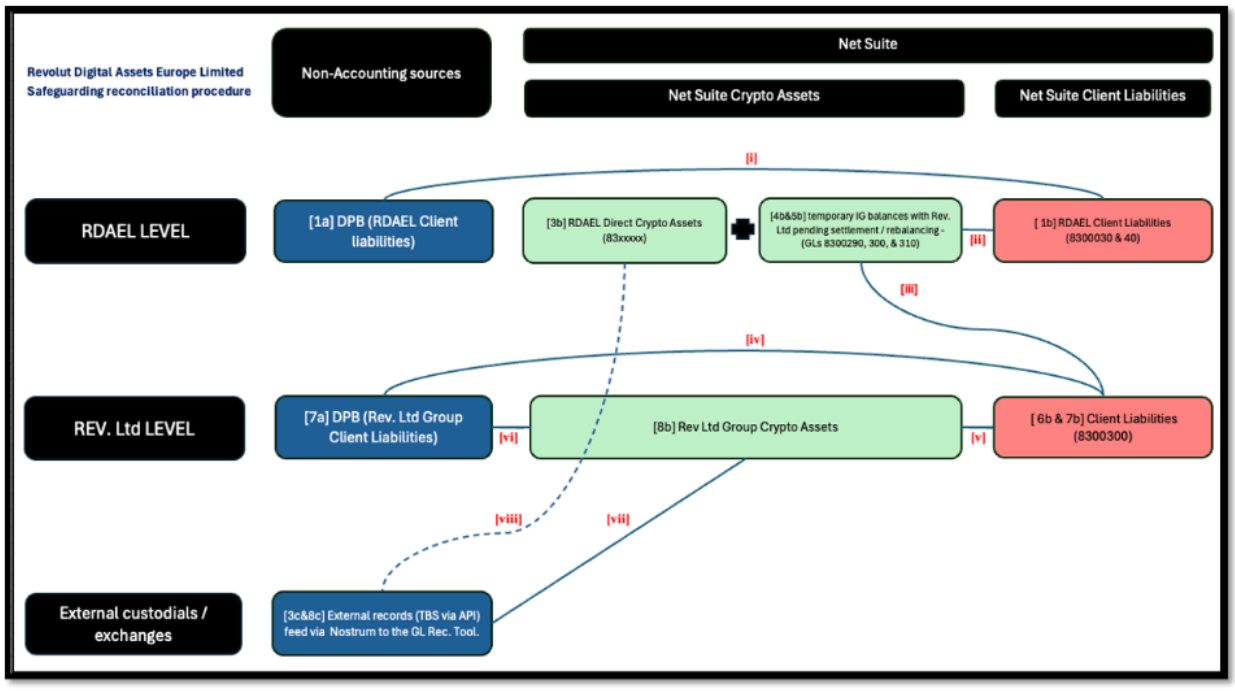
When funds are transferred between wallets, transaction fees may be applied to facilitate this movement. Because Revolut holds minimal crypto on its balance sheet, these transaction fees are paid from funds held in the wallet from where the transferred assets are held, i.e., clients' crypto-assets. On an intraday basis, in order to make these balances whole again, internal market making teams will perform a 'PNL swipe'. This involves buying the same amount of crypto that was used throughout the day to facilitate the movement of funds and crediting the account from where the fees were paid.

By way of example:

Revolut spends 0.0001 BTC on a transaction fee to move funds from an exchange to Fireblocks, with the above amount being debited from the exchange account. This 0.0001 BTC goes into PNL Swipe and, at a later time during the same day, Revolut buys 0.0001 BTC in the market to cover for the fact that it spent that small amount from the exchange account.

3.5 Reconciliation Procedures

See here the diagram of the full reconciliation cycle:



RDAEL reconciliations - performed

We perform the below reconciliations at RDAEL level:

No	Reconciliation description
[i]	Client liabilities: Accounting software balances vs DPB balances (The internal database of client liabilities)
[ii]	Client assets vs Client liabilities per the accounting software
[iii]	Crypto assets held by Rev. Ltd on behalf of RDAEL: Accounting software balance vs Balance per Rev. Ltd books
[viii]	Crypto assets held directly by RDAEL: Accounting software balance vs Treasury Balance Statements (TBS: Balances obtained by 3rd party custodians via API)

Revolut Group reconciliations - reviewed

No	Reconciliation description
[iv]	Client liabilities: Accounting software balance vs DPB balance (The internal database of client liabilities)
[v]	Client assets vs Client liabilities per the accounting software
[vii]	Crypto assets: Accounting software balance vs Treasury Balance Statements (TBS: Balances obtained by 3rd party custodians via API)

Responsibilities of Teams Involved

- Head of Custody: Responsible for performing monthly reconciliations, identifying discrepancies, and ensuring the accuracy of records.
- Compliance Team: Ensures that reconciliation processes comply with regulatory requirements and internal policies.
- Finance Team: Provides accurate records to support the reconciliation process and assists in resolving discrepancies.
- IT Team: Ensures that the systems used for reconciliation are secure, reliable, and functioning correctly.
- Risk Management Team: Ensures that Key Risk Indicators (KRIs) are sufficient to minimize risk and reviews each corrective action when it occurs.

Escalation Process

- Level 1 Escalation: Any discrepancy that cannot be resolved within five business days is reported to the Financial Controller. There is also a Key Risk Indicator in place to monitor any discrepancy between client liabilities and daily pocket balances.
- Level 2 Escalation: Discrepancies unresolved for more than five business days are escalated to the Head of Finance and Regulatory Compliance Manager.
- Level 3 Escalation: Discrepancies unresolved for more than 60 days require a verification report from Internal Audit once remediated.

In the event that a reconciliation discrepancy indicates a real shortfall in Client Assets, specifically where the issue cannot be attributed to timing, accounting, or operational errors but instead reflects missing client funds, this must be escalated immediately to the Group Financial Controller and Regulatory Compliance Manager. In addition, CySEC must be notified without delay in accordance with regulatory requirements.

Audit by Independent Third Party

- The reconciliation process is subject to an annual audit by an independent third party to ensure compliance with the policy and accuracy in financial reporting. The findings of this audit are presented to the Board of Directors.

M **anagement Information and Reporting**

- Board of Directors: Head of Custody provides monthly reports to the Board of Directors, summarizing the reconciliation activities, discrepancies identified, and resolutions.

Competency and Regulatory Awareness Framework

RDAEL maintains a structured framework to ensure that all relevant personnel possess and maintain the necessary knowledge, skills, and expertise to effectively carry out their responsibilities, including those related to client asset practices, in alignment with applicable regulatory expectations.

3.6 Client Statements

Accurate, complete and up-to-date statements of balances can be viewed by clients via the Revolut App and RevolutX and at any point in time.

3.7 Internal Materials

RDAEL - Business Continuity Management Policy (Including ICT) ; and
RDAEL Addendum - Outsourcing and Third Party Management Policy

3.8 Policy review

Policy reviewed frequency set to every 6 months to ensure that it remains accurate and up to date.

Related documents

There are no other documents linked to this one

Document version control

Version	Published on	Summary of changes	Additional info
1.0	02 Jan 2025	Initial version	
2.0	19 May 2025	Update to incorporate the OTC and OTP trading models	
2.1	19 May 2025	Added internal links	
3.0	02 Oct 2025	Update to incorporate the new custody arrangements, i.e. the bilateral (as opposed to tripartite) agreements between RDAEL and third party exchanges and the increased control over Fireblocks	
4.0	06 Nov 2025	Update for the temporary reconciliation procedures (section 3.5) until we are able to establish direct reconciliations of RDAEL balances to external custodians	
5.0	18 Dec 2025	Minor changes for going live in Fireblocks cold custody	
6.0	26 Mar 2026	• Updated the policy to reflect RDAEL's authorization as a MiCA-licensed crypto asset service provider. • Clarified that RDAEL client assets are segregated at the entity level, aligning with CySEC and MiCA requirements. • Enhanced details on reconciliation processes, including specific steps for RDAEL and Revolut Limited. • Strengthened third-party vendor oversight by requiring MiCA licensing and implementing annual attestations and KRIs. • Updated procedures for key recovery, emphasizing RDAEL employee initiation and	

		InfoSec's supporting role. • Refined the description of hot and cold wallet usage, emphasizing MiCA compliance for third-party exchanges and multi-signature requirements for cold storage.	
6.1	29 Sep 2026	• Updated references to internal policies and external regulations, including MiCA, with new links. • Changed the reporting frequency for the Head of Custody to the Board of Directors from quarterly to monthly.	
7.0	27 Oct 2026	• Updated the reconciliation process descriptions for RDAEL and Revolut Group. • Changed the title of the Revolut Limited reconciliations section to "Revolut Group reconciliations - reviewed". • Replaced the image displaying the reconciliation cycle diagram. • Removed reconciliation item [vi] from the Revolut Limited reconciliations.	
7.1	04 Nov 2026	• Added references to RBSA for clients who are French residents, ahead of the migration of those clients from RBUAB to RBSA.	