BOOK 6

Client Onboarding Through a Node

Title	**BOOK 6 Client Onboarding Through a Node**
Author	**Mr Denis Bouzon**
ORCID	**0009-0007-8894-8902**
Version / date	**1.0 28 September 2026**
Presentation page	**www.osnias-clearing.com/onboarding/**
Licence	**@Copyright Osnias-clearing** **Creative Commons Attribution 4.0 International**
DOI URL	**https://zenodo.org/uploads/23010805**

Executive summary

Book 6 describes the operational process through which a company becomes a participant of an Osnias Clearing node, funds an escrow contract with native EURC on Ethereum and gains access to the canonical clearing layer on Sei. It turns the identity, architecture, clearing, synchronization and security principles established in the preceding Books into a coherent admission, activation and exit process.

Keywords

Onboarding; node operator; EURC; USDC; Ethereum; Sei; escrow; Osnias-ID; KYB; AML; SEPA; self-custody; netting.

Core conclusion

The node operator is responsible for admission, the SEPA gateway and conversion from EUR to EURC and from EURC to EUR. The participant retains sole control of three independent seeds. Escrow release cannot be redirected by the operational EVM key alone: funds are released to the predefined cold EVM beneficiary.

Table of contents

1 Position within the document framework and status

Book 6 is a standalone document in the logical sequence of the Osnias Clearing document framework. It explains how the principles defined in Books 1 to 5 become an operational client journey for the participant and its node operator. It does not supersede any preceding rule; it brings those rules together at the operational entry point, from admission through offboarding.

Document	Function	Contribution to the onboarding journey
Book 1	Osnias-ID	Participant identity and crosschain linkages.
Book 2	Architecture	Separation of clearing, settlement and collateral.
Book 3	Clearing Rules	Obligations, netting, governance and responsibilities.
Book 4	Cycles and Calendar	Time synchronization and transaction states.
Book 5	Security	Domains A B C, composite condition and threat model.
Book 6	Onboarding	Admission, EUR/EURC gateway, escrow and exit.

Document status This document sets out a functional architecture and design requirements. It is not an independent audit, a formal verification, a penetration test, a security certification or an authorization for production deployment.

2 Architectural decisions

Principle	Application
Node responsibility	The node operator performs KYB and AML controls, verifies the bank account, provides the EUR/EURC gateway and is responsible for both the entry and exit processes.
Control retained by the participant	Seeds, private keys, recovery phrases, devices and backups remain under the participant’s exclusive control.
Three independent domains	A is the operational EVM signer, B is the independent Sei authorization and C is the predefined cold EVM beneficiary.
Native Ethereum	Collateral admitted in this journey is Ethereum-native EURC, without a bridge, wrapper or synthetic representation.
Canonical Sei	Sei carries the canonical clearing state and netting calculation. Ethereum locks the collateral and applies an authenticated outcome.
Non-custodial Osnias	Osnias Clearing receives neither euros, EURC nor private keys. It provides the rules, registries and position calculations.

Principle	Application
EOA-only	Addresses linked to the Osnias-ID are verified externally owned accounts. No third-party smart account constitutes the participant's identity.

2.1 Why Ethereum is the native escrow layer

Ethereum is selected as the native EVM network for escrow and collateral because of its decentralization, structural neutrality and mature security environment. It supports native USDC and EURC and provides liquidity depth suited to institutional requirements. The node operator or its regulated partner can therefore operate the EUR-to-EURC and USD-to-USDC gateways without a bridge, wrapper or synthetic representation.

The choice also reflects the absence of a single operator controlling the base layer. This characteristic reduces the escrow arrangement's dependence on any particular company and strengthens the continuity expected of collateral securing clearing obligations across multiple jurisdictions.

Network comparison As at 28 September 2026, Circle Mint supports USDC but not EURC on Arbitrum. Arbitrum therefore does not provide the direct EUR-to-EURC gateway required for this architecture. Base and Avalanche support both assets, but have a more concentrated institutional footprint: Base is developed by Coinbase, while Avalanche remains closely associated with Ava Labs and the Avalanche Foundation. These networks remain technically viable, but offer less structural neutrality for the role of reference escrow layer.

Transaction costs Ethereum fees may be higher than those on layer 2 networks or other EVM chains. This factor is not decisive in the Osnias architecture: Ethereum executes neither day-to-day payments, position calculations nor netting. It processes a limited number of collateral operations, primarily funding, any required freeze, release and exit. Operational volume remains on Sei. Ethereum costs therefore apply to a small number of escrow state transitions rather than to every transaction included in clearing.

3 Parties and responsibilities

Party	Primary responsibility
Participant	Generates and retains domains A, B and C, verifies signing intents, funds the escrow and decides on cryptographic renewal.
Node operator	Admits the participant, performs KYB and AML controls, verifies its bank account, performs or arranges EUR/EURC conversion and manages the client relationship.
Osnias Clearing	Defines the rules, coordinates cycles, maintains registry functions and calculates positions without holding the participant's assets or keys.
Ethereum escrow	Receives native EURC, applies cycle states, verifies the composite condition and releases funds only to registered beneficiary C.
Sei registry	Stores the canonical clearing state, independent authorization and individual and aggregate positions used for netting.
Verifier	Authenticates the Sei state submitted to the Ethereum contract under a finality, freshness, quorum and rotation policy that remains a trust boundary.
Regulated partner	Provides the node operator, where necessary, with institutional access to EURC issuance or redemption. The node operator remains responsible for the service provided to the participant.

4 Custody boundary

The node operator verifies addresses, signatures and states; it never receives the secrets used to produce them. Osnias Clearing does not hold, escrow, back up, recover or control any private key or recovery phrase. Osnias' non-custodial design does not remove the regulatory obligations applicable to the node operator or its partner when performing fiat conversions.

5 Security identity established during onboarding

Domain	Function	Requirement
A	Operational EVM signer	Ethereum EOA used for deposits and routine interactions. A hardware wallet is recommended. This key never determines a release destination on its own.
B	Independent Sei authorization	Address generated from a distinct seed. It authorizes an intent or canonical transition bound to the Osnias-ID, amount, beneficiary, nonce and expiry.
C	Cold EVM beneficiary	Ethereum EOA generated from a third seed and registered before release. It receives funds but does not sign during its cold receipt phase.

5.1 Seed independence

Domains A, B and C must originate from independent roots. Three addresses derived from the same BIP-32 seed do not constitute three security domains. No shared recovery phrase, derivation root or backup may be used. In an institutional deployment, separation may be evidenced through key-generation ceremonies, HSMs or distinct custody domains.

Address C The onboarding procedure must not require cold address C to sign a routine transaction. The participant provides its public address and confirms its backup procedure in accordance with the node operator's controls; the private key and recovery phrase remain offline.

5.2 Linkage through Osnias-ID

Osnias-ID links the admitted company, its node, domains A, B and C, the currency and the cycle profile. It is not a cryptographic key. Linkages must remain consistent across the registries, and any discrepancy must block activation or release.

6 Onboarding journey

The journey links the node operator's fiat gateway, the participant's three independent domains and the two onchain registries. The upper flow represents entry into EURC and escrow funding; the central flow carries the canonical authorization; and the lower flow represents secure release and redemption.

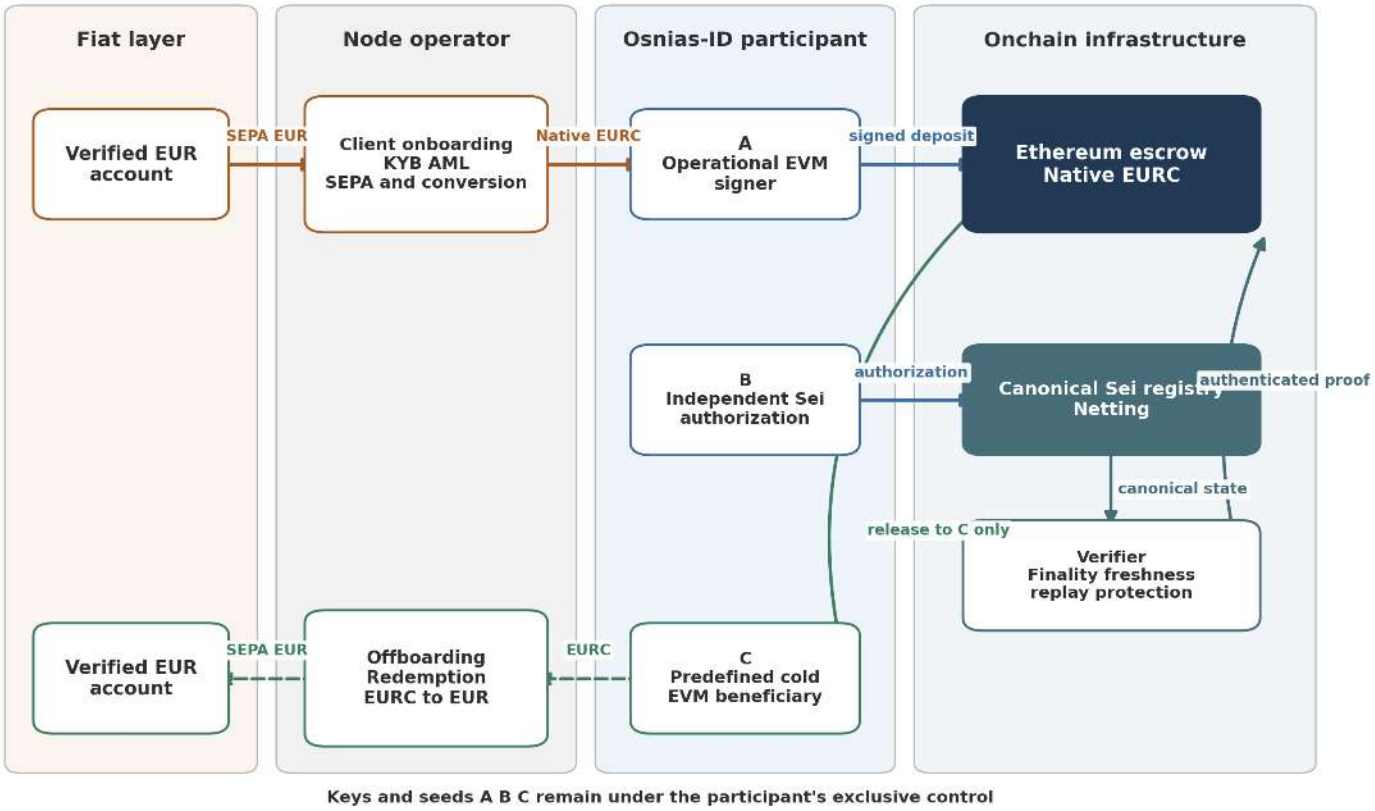

Figure 1 Onboarding journey and release condition

6.1 Operational sequence

Step	Phase	Expected outcome
1	Admission	The node operator identifies the company, its representatives and beneficial owners, verifies the bank account and applies its KYB and AML procedures.
2	Domain creation	The participant generates A, B and C separately in appropriate environments and retains sole control of secrets and backups.
3	Proofs and registration	A and B prove control through domain-separated challenges with a unique nonce and expiry. C is registered as the cold beneficiary without being used as a routine signer.
4	Osnias-ID	The node operator links the admitted identity, its own identifier, the three domains, the currency and the cycle profile in the authorized registries.
5	EUR/EURC conversion	The participant transfers euros through SEPA. The node operator performs or arranges the conversion and delivers Ethereum-native EURC to verified address A.
6	Ethereum deposit	The participant authorizes and signs the EURC deposit into the escrow contract linked to its Osnias-ID and node.
7	Activation	The system verifies the official token, linkages, beneficiary C, cycle state, finalized amount and absence of discrepancies between registries.

6.2 Minimum activation requirements

- KYB and AML controls approved by the node operator;
- bank account held in the participant's name verified;
- active Osnias-ID linked to the correct node, currency and cycle profile;
- domains A, B and C registered with roots declared to be independent;
- address C fixed as the release beneficiary before any clearing exposure;
- Ethereum-native EURC deposited and the transaction finalized;
- clearing capacity limited to collateral recognized as eligible;
- fail-closed control for any inconsistent, incomplete or stale state.

7 Ethereum escrow and release condition

The escrow contract technically links the participant to its node operator without granting the operator discretionary withdrawal authority. It locks native EURC, publishes events relevant to evidence of solvency and applies the state transitions permitted by the cycle. Effective enforcement remains to be demonstrated through code and testing.

7.1 Authorization payload

Category	Minimum content
Domain	Protocol version, domain separator, Osnias-ID and source and destination chain identifiers.
Contracts	Escrow address, verifier address and official Ethereum-native EURC contract address.
Transaction	Currency code, cycle or mode, amount, unique nonce, timestamp and expiry condition.
Canonical state	Sei state reference, authorization or transaction identifier and required finality level.
Destination	Exact commitment to the pre-registered beneficiary C.

7.2 Composite release condition

- valid Osnias-ID and consistent linkages in the applicable version;
- cycle state permitting release and no active or disputed obligation;
- authorization B or canonical Sei state authenticated by the verifier;
- finality, freshness, quorum and reorganization policy requirements satisfied;
- nonce or proof not previously consumed and exact match of amount, asset and contracts;
- destination strictly equal to the registered cold beneficiary C.

Destination invariant Compromise of key A must not allow C to be replaced by an address selected at the time of release. No single administrative path may bypass this condition.

8 Netting and integration with Sei

The Ethereum escrow does not calculate netting. Individual positions are calculated and consolidated on Sei, then aggregated by node to determine net obligations and the inter-node residual. Ethereum receives only the canonical outcome required to freeze, settle or release collateral.

- the sum of all positions in the cycle remains equal to zero;
- clearing capacity does not exceed the EURC collateral recognized as eligible;
- each individual outcome reconciles with the node aggregate;
- post-clearing mirror reconciliation aligns the canonical Sei state with the final Ethereum escrow state;
- only the residual remaining after internal node netting is exposed to inter-node settlement;
- any discrepancy between registries blocks new transactions until reconciliation.

9 Offboarding burn and collateral release to the bank account

1. The participant requests exit from registered domain A.
2. The system verifies that no amount is frozen, disputed or allocated to an active obligation.
3. The composite condition is verified, including authorization B or the authenticated Sei state and replay protection.
4. The contract releases EURC exclusively to predefined cold address C.
5. The participant then transfers EURC from C to the redemption address provided by the node operator.
6. The node operator performs or arranges the EURC-to-EUR conversion and transfers the euros to the verified bank account.
7. Once all remaining positions have been settled, the identity moves to SETTLED and then irreversibly to REVOKED.

Consequence of using C As soon as address C signs a transfer of received funds, it leaves its cold phase. If the participant remains in the system following a partial release, a new cold beneficiary must be registered through a protected renewal procedure.

10 Identity and escrow states

Object	State	Effect
Identity	PRE-ENROLLED	Admission in progress; no clearing capacity.
Identity	ACTIVE	A B C linkages validated and exposure authorized within collateral limits.
Identity	RENEWAL PENDING	New identity prepared; the previous identity cannot increase its exposure.
Identity	MIGRATION	Positions and funds are transferred or settled under enhanced controls.
Identity	SETTLED	No position or obligation remains.
Identity	REVOKED	Irreversible final state; history retained for audit.
Escrow	FUNDED ELIGIBLE	EURC finalized and amount recognized as potential capacity.
Escrow	FROZEN CONTESTED	Amount unavailable during calculation or dispute.
Escrow	CLEARED RELEASABLE	Authenticated outcome; amount releasable only to C.

11 Controls and risks to be addressed

Risk	Required treatment
Shared root	A shared BIP-32 seed defeats A B C separation. Procedural controls and institutional evidence are required.
Blind B signature	The displayed intent must bind the Osnias-ID, asset, amount, beneficiary, nonce and expiry in a human-readable format.
C substitution	The contract rejects any destination other than the registered beneficiary and governs beneficiary renewal separately.
Replay or substitution	The proof is single-use and bound to the chain, contract, cycle, amount and beneficiary.
TOCTOU divergence	A registry version or immutable commitment is fixed; any divergence between verification and execution blocks the transaction.
Verifier	Authentication, finality, reorganizations, quorum, rotation and stale states must be specified, implemented and tested.
Administrative authority	No single upgrade, registry or emergency key may unilaterally modify the composite condition or beneficiary.
EURC freeze	The issuer’s compliance powers remain applicable; the contract cannot override a token freeze.

12 Contractual and regulatory allocation

The node operator contracts with the participant and is responsible for onboarding, offboarding, identity controls, the SEPA gateway and EUR/EURC conversion. It must hold the required authorizations or engage an appropriately authorized regulated partner. The precise scope depends on its jurisdiction and contractual arrangements.

Function	Responsible party
KYB and AML admission	Node operator
Bank account and SEPA	Node operator or its regulated partner
EUR/EURC conversion	Node operator or its regulated partner
Control of seeds A B C	Participant exclusively
Collateral escrow	Ethereum contract
Canonical state and netting	Osnias Clearing on Sei
Crosschain authentication	Verifier under a defined governance framework
Settlement of the outcome	Nodes under the Clearing Rules
Offboarding and redemption	Node operator

13 Acceptance invariants

- no participant seed or private key leaves its control domain;
- neither the node operator nor Osnias can independently initiate a transaction from A, B or C;
- A, B and C originate from independent roots and perform distinct functions;
- the escrow accepts only the officially configured Ethereum-native EURC;
- the Ethereum escrow never calculates netting;
- the outcome applied on Ethereum originates from an authenticated Sei state bound to the active cycle;
- no withdrawal is possible during a freeze, dispute or active obligation;
- every release is made to C and never to a destination supplied at the time of release;
- post-clearing reconciliation aligns Sei positions, node aggregates and Ethereum balances;
- the REVOKED state permanently prevents any new exposure while preserving the audit history.

14 Interface with Book 5 Security

Book 5 remains the normative reference for the controls protecting this journey. It addresses, in particular, the insufficiency of any single key, the independence of domains A B C, the composite release condition, registry integrity, replay protection, renewal and revocation. This Book 6 applies those requirements to the client journey without duplicating their security analysis. Implementation evidence, adversarial testing and independent review remain necessary before production deployment.

15 Conclusion

Book 6 completes the Osnias Clearing document framework with its operational execution layer. The node operator manages the client relationship, admission and the EUR/EURC gateway; the participant retains exclusive control of domains A B C; Ethereum escrows native EURC; and Sei carries the canonical clearing state and netting. This allocation preserves the separation of responsibilities, self-custody of keys and verifiability of collateral while providing an entry and exit process consistent with the preceding Books.