

Book 3

Clearing Rules

Title	<u>Book 3</u> Clearing Rules
Author	Mr Denis Bouzon
ORCID	0009-0007-8894-8902
Release / date	1.3; 14 October 2026
Landing page	https:// www.osnias-clearing.com/rules/
Licence	© Osnias Clearing Published under Creative Commons Attribution 4.0 International (CC BY 4.0)
URL DOI	https://zenodo.org/records/22922199

Abstract

Osnias Clearing defines a multilateral clearing framework based on deterministic and auditable rules.

The architecture strictly separates clearing calculation, risk controls and settlement execution.

Clearing positions are held natively in the canonical Sei position ledger and backed 1:1 by EVM escrows: no clearing token is issued.

Node operators remain responsible for settlement escrow control, custody of funds and execution of settlement.

Controls rely on a Time Oracle, a strictly positive net position condition on every obligation, a real-time chamber solvency control built on two oracles (Ethereum escrow, Sei net positions) and post-clearing reconciliation.

The paper benchmarks the architecture against PFMI, ISO 20022, settlement finality and applicable regulatory requirements.

Keywords

Multilateral clearing · Netting · Settlement · PFMI · ISO 20022 · Time Oracle · Solvency · Escrow · Position ledger · Sei · EVM · Finality · Auditability

Table of contents

I Position within the document corpus and status.....	3
II Executive summary.....	3
II.a Closing period sequence (at the end of the selected 1W / 9W / 13W cycle).....	4
II.b Solvency and evidence.....	4
II.c Clearing / settlement separation.....	5
II.d Structural invariants.....	5
II.e Member admission and network topology carried by Osnias-ID.....	6
II.f Regulatory perimeter and qualification.....	6
III INTERNATIONAL STANDARDS AND REFERENCE FRAMEWORKS.....	7
III.a CPMI-IOSCO PFMI.....	7
III.b CLS as an operational benchmark.....	7
III.c ISO 20022 — Messaging, not settlement finality.....	7
III.d Human-readable statements and machine-to-machine messages.....	8
III.e Accounting offset vs operational clearing.....	8
IV APPLICATION TO THE OSNIAS NETWORK.....	8
IV.a Functional roles.....	8
IV.b Time Oracle and standard clearing-cycle profiles.....	9
IV.c P2P freeze and canonical snapshot.....	9
IV.d Per end-user state computation.....	10
IV.e Node-level aggregation and chamber conservation.....	10
IV.f Per-node escrow integrity check.....	10
IV.g Key clarification — internal netting alone does not change RN.....	11
IV.h Disputes and finalisation.....	11
IV.i Settlement-escrow availability of paying nodes.....	11
IV.j Inter-node settlement.....	11
IV.k Internal allocation by the receiving node.....	12
IV.l Network fees.....	12
IV.m Four distinct finality states.....	13
IV.n Exception handling and node default.....	13
IV.o Post-clearing mirror reconciliation.....	14
IV.p On-ledger data and the purpose field.....	14
IV.q Clearing position ledger and real-time solvency control.....	14
IV.r Administration keys and powers.....	16
IV.s Main risks.....	16
V CYCLE CLOSING PERIOD: WHO DOES WHAT, WHEN.....	17
V.a Chronological workflow.....	19
V.b Architecture and controls overview.....	20
VI REGULATORY AND TECHNICAL CONTROL MAPPING.....	21
VI.a Audit file.....	21
VII CHAMBER INTEGRITY & CONSERVATION ORACLE AND PARTICIPANT TRANSPARENCY.....	22
VII.a Purpose and scope of the Chamber Integrity & Conservation Oracle.....	22
VII.b 1:1 chamber-level conservation invariant.....	24
VII.c Real-time monitoring, five-minute attestation and freshness.....	24
VII.d Interaction with the Time Oracle and the position-ledger contract.....	24
VII.e Transparency on the end-user platform.....	24
VII.f Oracle failure model.....	25
VII.g Audit and PoC test requirements.....	25
VII.h Updated control chain.....	26

VIII Open points for legal counsel.....	26
IX Regulatory bibliography.....	27

I Position within the document corpus and status

Book 3 is a standalone document within the logical continuity of the Osnias Clearing corpus.

Document	Function	Contribution to the framework	URL
Book 1	Osnias-ID	Participant identity and crosschain linkages.	https://www.osnias-clearing.com/osniasid/
Book 2	Architecture	Separation of clearing, settlement and collateral.	https://www.osnias-clearing.com/architecture/
Book 3	Clearing Rules	Obligations, netting, governance and responsibilities.	https://www.osnias-clearing.com/rules/
Book 4	Cycles and Calendar	Time synchronization and transaction states.	https://www.osnias-clearing.com/cycle/
Book 5	Security	Domains A B C, composite condition and threat model.	https://www.osnias-clearing.com/security/
Book 6	Onboarding	Admission, EUR/EURC gateway, escrow and exit.	https://www.osnias-clearing.com/onboarding/
Book 7	O-POP Osnias	Mainnet access architecture, dedicated RPC and audit traces.	https://www.osnias-clearing.com/pop/

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 a go-live authorisation.

II Executive summary

Osnias decouples clearing computation from settlement execution. Osnias computes and records clearing obligations; each NNN node operator retains exclusive authority over settlement-escrow control, custody of funds and payment execution. This page summarises the core invariants, the cycle closing period, the solvency controls and the evidence model intended for external stakeholders.

Major architectural simplification (Release 1.3). Osnias no longer issues a clearing token. Each member's clearing capacity is recorded natively as a position in the canonical Sei ledger: at cycle open, the position equals the amount held in the member's EVM escrow, frozen for the whole cycle; every accepted obligation atomically books -X on the debtor and +X on the creditor. MINT and BURN operations, the token contract and the associated issuance authority are removed. Solvency is carried by the ledger state itself, enforced ex ante on every write and monitored in real time by the chamber solvency control (§4.q and §7). The token becomes redundant once this control directly compares the Sei net total (position oracle) with the Ethereum escrow total (escrow oracle, relayed through the Controllers) (full rationale in §4.q).

Core invariant	Operational scope
Clearing $\neq$ settlement	Osnias computes and records obligations; node operators execute monetary settlement.
No custody by Osnias	Osnias holds no ownership, custody or unilateral disposal right over settlement funds.
Single canonical snapshot	All cycle computations use the same identified EVM/Sei reference states.
Fail-closed controls	A missing authorisation, a material unresolved exception or a stale/failed solvency proof blocks the action concerned.
Node sovereignty	Each NNN node operator controls its accounts, its settlement-escrow workflow and its banking/payment relationships.
Contractual membership and topology	Each member is admitted by contract with its local node; a node is identified by its network-node pair (KK, NNN); Osnias-ID provides the addressing and topology layer.

II.a Closing period sequence (at the end of the selected 1W / 9W / 13W cycle)

UTC	Phase	Owner
Friday 23:59:59	P2P ends: last order accepted	Time Oracle
Saturday 00:00	P2P closed (until the end of the adjustment phase) and canonical snapshot	Time Oracle / Clearing Engine
Saturday, before 06:00	Dated statements: users (published by nodes, sent to clients); nodes (consolidated by Osnias, sent to node managers)	Node operators / Osnias
Saturday–Sunday	Full-day freeze: dispute window	Users / node managers
Sunday 23:59	Disputes closed; final net dated statements; $\Sigma RN = 0$	Clearing Engine / node operators
Monday (day 1, netting)	Client escrows aligned with the net dated statement, then inter-node balancing; no movement to an Osnias account	Node managers and operators
Tuesday (1W); Tuesday–Thursday (9W, 13W)	Adjustment phase: the client freely adjusts its escrow (withdrawal to the withdrawal address or top-up)	Clients
Wednesday 00:00 (1W); Friday 00:00 (9W, 13W)	Escrowed amount frozen and booked as opening position $Pu(0) = Cu$; P2P reopens; fee orders from the completed cycle written first	Time Oracle / ledger contract / Clearing Engine

II.b Solvency and evidence

In real time, the chamber solvency control compares the escrow total on the Ethereum side, computed by the escrow oracle and relayed to Sei through the Controllers, with the total of net balances on the Sei side, computed by the position oracle; the difference must be zero at all times. A signed attestation is published every five minutes, without controlling funds or the cycle calendar. In addition, a member's net position on Sei can never be zero or negative: a member can only validate an ISO 20022 request if its net position is sufficient to cover it (§4.q). This

condition limits each debtor client's exposure to its own collateral; the settlement risk borne by a creditor client during the netting phase is addressed in §4.q. Node positions may be positive or negative during normal P2P activity. End-user statements, fee invoices, disputes, settlement references, post-clearing mirror checks and oracle attestations are retained as auditable evidence.

Time Oracle = time authority

Escrow oracle (Ethereum) + position oracle (Sei) = chamber solvency control | Clearing Engine = computation | NNN node operator = settlement-escrow control and settlement execution.

II.c Clearing / settlement separation

Osnias Clearing rests on a structural separation between clearing and settlement. Osnias computes, records and communicates clearing states and settlement obligations. It does not hold, control, transfer or dispose of settlement funds. Each NNN node remains under the exclusive authority and responsibility of its owner/operator for settlement-escrow control, custody, banking relationships and execution of inter-node payments.

The clearing process halts P2P activity, locks a reproducible blockchain snapshot, computes the delta between each end-user's EVM escrow state and its clearing position on the Sei ledger, aggregates these deltas per node, opens a dispute window, finalises node positions, confirms settlement-escrow availability for paying nodes, and only then releases settlement obligations to node operators.

International standards are used as design benchmarks, not as a self-declaration of legal status or regulatory compliance. Regulatory qualification is a matter for the competent authority in the relevant jurisdiction.

II.d Structural invariants

Invariant	Rule
Clearing $\neq$ settlement	Osnias computes and records clearing obligations; node operators execute settlement.
No custody by Osnias	Osnias holds no ownership, custody or unilateral disposal right over settlement funds.
Node-operator sovereignty	Each NNN node owner/operator controls its accounts, its settlement-escrow arrangements and the execution of its payments.
P2P fail-closed	Absent explicit authorisation, the P2P order is rejected.
Single snapshot	All clearing computations in a cycle use the same canonical block reference.
Deterministic aggregation	Each node position is the exact algebraic sum of the final deltas of the end-users attached to that node.
Settlement-escrow availability before settlement	No paying-node instruction is released until the corresponding amount is proven available in the escrow under the node operator's control.
Receipt before receiving-node allocation	A receiving node performs its internal allocation only after actual receipt of settlement funds.
External settlement rail	Monetary settlement takes place over the payment rail selected and controlled by node operators.
UTC-only cycle	All operational clearing deadlines are defined in UTC.
Permissioned contractual membership	No wallet becomes a chamber member through a mere technical connection; membership requires a signed contract with the relevant local node.

II.e Member admission and network topology carried by Osnias-ID

Osnias Clearing operates as a federated, permissioned network. An end-user becomes a member of a clearing chamber only under a client/clearing agreement signed with the relevant local node. The member is therefore contractually attached to the local node; connecting a wallet does not constitute admission.

Each local node is a local operating entity acting within its applicable regulatory and supervisory perimeter. It remains responsible for the member relationship, onboarding, local controls, settlement-escrow arrangements and settlement execution.

Node licensing requirement. On Monday, the local node adjusts its clients' EURC escrows and transfers inter-node amounts. These operations may constitute crypto-asset services provided on behalf of clients within the meaning of Regulation (EU) 2023/1114 (MiCA), in particular custody and transfer, and, since EURC is an e-money token, payment services within the meaning of Directive (EU) 2015/2366. Admission of a node is therefore conditional on proof that it holds the authorisations required in its jurisdiction, or falls under a documented exemption. In France, this requires crypto-asset service provider authorisation from the AMF, the transitional period having ended on 1 July 2026, together with payment institution or e-money institution status, or agent status of such an institution, with the ACPR.

Client categories. The 9W profile is reserved for commercial obligations between professionals. Where the 13W profile admits natural persons acting for non-professional purposes, the local node MUST apply the applicable consumer-protection rules and the requirement for clear, fair and not misleading communication, including for information on fees and risks (§4.s).

Network governance rules (Rulebook, technical standards, clearing rules, interoperability requirements and node admission) are maintained by the network governance entity, which does not hold members' or nodes' settlement funds. The legal structure and contractual topology are covered in Book 5 – Legal Qualification Memorandum.

Node identity: a node is identified by the network-node pair (KK, NNN) of its Osnias-ID. Since a clearing chamber may bring together nodes from several networks (up to 99 networks × 999 nodes), a node's identity is never assessed on the NNN field alone.

Osnias-ID is not merely a technical identifier. It is the addressing and topology layer of the clearing network: the namespace used to locate and link clearing chambers, networks, nodes, currencies, cycle profiles and members. Functionally, it plays for Osnias Clearing a role analogous to TCP/IP addressing in a communications network.

II.f Regulatory perimeter and qualification

This document deliberately refrains from qualifying Osnias itself as a payment system, financial market infrastructure, central counterparty (CCP), settlement system or any other regulated category, or from ruling out such a qualification. That qualification depends on applicable law, the facts, the jurisdiction, the contractual arrangements and the role actually performed by each entity.

For the Swiss analysis, FINMA notably identifies payment systems as arrangements for clearing and settling payment obligations. Accordingly, the functional separation described in this document must be presented as an architectural fact, not as a legal conclusion on the regulatory perimeter.

For the European Union and France, the authorities potentially concerned include: the AMF, for crypto-asset services (MiCA); the ACPR, for payment services and the issuance or distribution of e-money, including where they concern e-money tokens; and the Banque de France, for payment-system oversight and any designation of a system for settlement-finality purposes (Article L.330-1 of the French Monetary and Financial Code). This document does not prejudge any of these qualifications.

Recommended wording: regulatory qualification is deliberately left to the competent authority. Osnias functionally separates the computation of clearing positions from the execution of monetary settlement over external payment rails. The preliminary qualification analysis is set out in Book 5 – Legal Qualification Memorandum.

III INTERNATIONAL STANDARDS AND REFERENCE FRAMEWORKS

III.a CPMI-IOSCO PFMI

Reference	Control objective	Osnias response
P1 — Legal basis	Clearly defined rules, rights, obligations and enforceability.	Rulebook, node agreements, dispute rules and finality definitions.
P3 — Risk management	Identify and manage material risks.	Segregate clearing, settlement-escrow, settlement, oracle and operations controls.
P4 — Credit risk	Control participant exposures.	Net position on Sei always strictly positive: no ISO 2022 request validated without a sufficient net position, each debtor client's exposure limited to its own collateral; paying-node settlement risk during netting governed by the Rulebook (§4.q). No paying-node instruction is released before settlement-escrow availability is confirmed.
P7 — Liquidity risk	Monitor and manage the liquidity required for settlement.	Paying-node settlement-escrow availability confirmed before settlement.
P8 — Settlement finality	Define final settlement and the point of irrevocability.	Distinguish computation finality, instruction irrevocability, settlement finality and cycle close.
P9 — Money settlements	Control settlement-asset and settlement-bank risk.	Use external payment rails under the responsibility of node operators.
P13 — Default	Have clear rules for participant default.	Settlement-escrow unavailability / payment failure puts the node into a fail-closed exception state.
P17 — Operational risk	Resilience, recovery and operational controls.	Replayable snapshot, logs, oracle checks and exception handling.
P22 — Communications	Use or accommodate internationally accepted standards.	ISO 2022 where the selected settlement rail supports it.
P23 — Transparency	Clear and comprehensive rules and procedures.	Published cycle calendar, fee base, dispute and exception rules.

III.b CLS as an operational benchmark

CLS is used solely as an operational benchmark for step sequencing, settlement-availability discipline and finality concepts. Its legal and economic architecture is not equated with that of Osnias.

The relevant lesson concerns sequencing: a computed obligation must not automatically become an executable settlement instruction before the required settlement-escrow availability is confirmed.

Computed obligation → settlement availability confirmed → payment instruction → settlement confirmation

III.c ISO 2022 — Messaging, not settlement finality

ISO 2022 is a financial messaging standard. It does not itself execute a payment, provide liquidity, set banking cut-off times or guarantee settlement finality by a given deadline.

Message	Name	Potential use in Osnias
pacs.009	FinancialInstitutionCreditTransfer	Primary candidate for node-to-node institutional payment instructions, subject to the settlement rail's implementation guide.
pacs.002	FIToFIPaymentStatusReport	Status report, acceptance or rejection.
pacs.004	PaymentReturn	Return flow where supported by the relevant payment community.
pacs.028	FIToFIPaymentStatusRequest	Payment status request where confirmation is delayed or missing.

The exact message versions and usage profile MUST comply with the Rulebook and the implementation guide of the selected settlement rail or banking community. Osnias must not independently impose a message version incompatible with the receiving rail.

III.d Human-readable statements and machine-to-machine messages

End-user and node clearing statements may be rendered as PDFs for human review. Such PDFs do not, by themselves, constitute ISO 20022 settlement messages.

Recommended architecture: the PDF clearing statement is bound to the structured clearing record by the cycle ID, the Osnias-ID, the document ID and its cryptographic hash. ISO 20022 is then used for machine-to-machine messaging related to funding and settlement where the payment rail supports it.

Clearing statement = PDF + structured record + hash binding

Settlement messaging = ISO 20022 profile of the selected rail

III.e Accounting offset vs operational clearing

Operational clearing netting must remain distinct from accounting offset in financial statements. A clearing result produced by Osnias does not automatically determine the accounting presentation of a participant's assets and liabilities.

Each participant remains responsible for its own accounting treatment under the applicable framework, including the conditions for accounting offset.

IV APPLICATION TO THE OSNIAS NETWORK

IV.a Functional roles

Actor / layer	Responsibility
Sei clearing ledger	Canonical state of members' clearing positions; no clearing token is issued (§4.q).
EVM escrow layer	Escrow / settlement-availability state associated with end-users and nodes.
Time Oracle	External time authority. The position-ledger contract queries it before any action to determine the current phase (FREEZE, NETTING, ADJUSTMENT, P2P). It applies the chamber's cycle profile (1W, 9W or 13W) and returns the applicable OPEN/CLOSED or ALLOW/DENY state; the ledger contract does not embed the cycle calendar itself.

Actor / layer	Responsibility
Clearing Engine / Oracle	Reads states, computes deltas, aggregates node positions, applies clearing rules and produces obligations; on Saturday, publishes the consolidated dated node statement and sends it to node managers.
End-user	Reviews the computed statement and may dispute it within the designated window.
NNN node operator	Holds/controls node accounts and settlement-escrow arrangements; on Saturday, publishes its users' dated statements and sends them to its clients; on Monday, aligns its clients' escrows and executes inter-node balancing.
Node operator (KK, NNN) — manager key (netting)	Exclusive authority, on Monday (netting phase), to adjust the escrows of clearing accounts attached to its own network-node pair only, using a manager key or multisig setup under its exclusive control. Its movements are limited to the node's users and to the node account for inter-node amounts; outside the netting phase, this key has no effect on escrows. It creates no position: the opening position is booked from the escrowed amount observed on the EVM side at the start of the P2P period. This authority is bounded by the protocol controllers: Osnias-ID / escrow / chamber consistency, Time Oracle authorisation, chamber conservation invariant and node integrity check. Osnias holds no key allowing it to adjust an escrow.
Bank / settlement rail	Executes the actual monetary transfers.
ISO 20022 interface	Carries payment/status messages where the settlement rail supports it.
Chamber Integrity & Conservation Oracle (solveny control)	Chamber-level solveny control made of two oracles: the escrow oracle, on the Ethereum side, reads the escrow contracts, totals them and relays the total to Sei through the Controllers; the position oracle, on the Sei side, reads each member's net balance and totals them. The control requires Sei net total = Ethereum escrow total, with zero difference at all times, and publishes a signed attestation every five minutes. It does not assess node-by-node solveny and moves no funds.

IV.b Time Oracle and standard clearing-cycle profiles

The position-ledger contract is deliberately minimal. It does not compute calendar dates nor determine the current cycle phase itself. Before any time-gated operation, the contract queries the external Time Oracle and executes the action only if the oracle returns the required authorisation.

The standard chamber profiles are 1W (testnet), 9W (B2B commercial obligations) and 13W (eligible non-commercial obligations), in accordance with Book 4 (Release 2.2). The selected profile defines the operating cycle of the chamber concerned. The closing period described in §2.a and section 5 (P2P closed from Saturday 00:00 until the end of the adjustment phase: Tuesday 23:59 in 1W, Thursday 23:59 in 9W and 13W) takes place at the end of the selected cycle; it is not a daily economic cycle.

Ledger action → Time Oracle(profile) → ALLOW / DENY → execute / reject

This separation keeps the ledger contract compact and lets time rules evolve independently of the ledger's execution logic.

IV.c P2P freeze and canonical snapshot

At 00:00 UTC on the clearing date determined by the Time Oracle's 1W, 9W or 13W profile, the position-ledger contract queries the Time Oracle. As soon as the oracle returns DENY for P2P, the contract rejects new P2P orders and the closing period begins. The contract does not determine this date itself. The last P2P order of the

cycle is accepted on the Friday of the final week at 23:59:59 UTC; P2P is then closed from Saturday 00:00 until the end of the adjustment phase (Tuesday 23:59 UTC in 1W; Thursday 23:59 UTC in 9W and 13W). Saturday and Sunday are two full freeze days.

Snapshot = (block height, block hash)

The freeze ensures that the state used for end-user and node computations cannot be altered by new P2P activity.

IV.d Per end-user state computation

For each end-user u , the delta between the clearing-eligible escrow principal attributable to that end-user on the EVM side and its clearing position on the Sei ledger (§4.q) is computed deterministically from the canonical snapshot; it appears in the dated statement that the home node publishes and sends to the user.

$$\Delta u = \text{EligibleEscrowEVM}(u) - \text{PositionSei}(u)$$

Since $\text{PositionSei}(u) = \text{EligibleEscrowEVM}(u) + \text{accepted receivables} - \text{accepted payables}$, it follows that $\Delta u = \text{accepted payables} - \text{accepted receivables}$: Δu is exactly the end-user's net obligation position over the cycle. The sign convention is unchanged ($\Delta u > 0$: net debtor).

For the avoidance of doubt, the “eligible escrow” value used in the clearing equation must exclude any buffer, reserve, fee amount or collateral component that is not part of the reconciled clearing principal. This prevents structural over-collateralisation from creating a false clearing imbalance.

The exact taxonomy of EligibleEscrow components MUST be defined in the technical Rulebook. Each included or excluded component must be identifiable from a deterministic contract state or signed source data, and reproducible from the cycle audit file. At a minimum, buffers, reserves, fee balances and collateral not attributable to the clearing principal must be classified separately and excluded from the EligibleEscrow value, unless the Rulebook expressly provides otherwise.

$$\text{EscrowTotal} = \text{EligibleEscrow} + \text{Buffer} + \text{Reserve} + \text{FeeBalance} + \text{OtherNonClearingAmounts}$$

Δu may be positive, negative or zero. The clearing process records the delta; it does not require each end-user to be individually balanced.

IV.e Node-level aggregation and chamber conservation

$$RN = \sum \Delta u \text{ over all end-users } u \text{ attached to node } N$$

RN is the node's aggregate clearing position under the convention $\Delta u = \text{EligibleEscrowEVM}(u) - \text{PositionSei}(u)$. $RN > 0$ identifies a settlement-paying node; $RN < 0$ identifies a settlement-receiving node; $RN = 0$ requires no inter-node settlement.

The chamber-wide conservation check is performed on the same clearing perimeter and with the same definition of eligible escrow principal.

$$\sum RN = 0$$

A non-zero result is a reconciliation exception. The cycle must not produce final settlement instructions until the discrepancy is identified and resolved.

IV.f Per-node escrow integrity check

The chamber solvency control (Ethereum escrow oracle and Sei position oracle) checks chamber-wide 1:1 conservation in real time. Separately, each node is subject to an escrow integrity check, without requiring its RN to be zero during the P2P phase.

$$\text{EscrowN}(t) = \text{EscrowN}(t_0) + \text{DepositsN} - \text{WithdrawalsN} + \text{SettlementInN} - \text{SettlementOutN}$$

Any unexplained change in a node's escrow outside authorised adjustments (Monday netting, adjustment phase) or settlements is an integrity exception. This check pinpoints the source of a discrepancy without creating a false node-level solvency default.

Execution and cadence. The check is run by the Clearing Engine / attestation controller every five minutes and immediately after each relevant adjustment or settlement event affecting the node's escrow.

Effect of the check. Any unexplained escrow change puts the node concerned into EXCEPTION state, blocks any new adjustment for that node and retains the computation and event data in the audit trail. This node-level integrity exception is distinct from the chamber's overall solvency status.

IV.g Key clarification — internal netting alone does not change RN

A redistribution or netting between end-users of the same node does not, by itself, change the algebraic sum RN. It changes the internal allocation of positions, not the node's aggregate exposure to the network.

Consequently, internal netting within a paying node is a local allocation step. It does not change RN by itself. The inter-node amount to transfer remains RN for a paying node ($RN > 0$), absent a new external economic event changing the node's position.

Internal redistribution $\Rightarrow$ RN unchanged

This distinction is essential to prevent double counting or the appearance that a node shortfall could disappear through mere internal entries between its end-users.

IV.h Disputes and finalisation

On Saturday morning, before 06:00 UTC, each node publishes its users' dated statements and sends them to its clients. For its part, Osnias produces a consolidated dated statement of the nodes and sends it to node managers. Users and node managers have Saturday and Sunday, two full freeze days, to raise disputes.

Disputes are reviewed as the window runs. At its close, on Sunday at 23:59 UTC, the net dated statements of users and nodes are finalised and $\Sigma RN = 0$ is verified.

A material unresolved dispute affecting the node's position at the settlement cut-off prevents the settlement instruction concerned from being treated as final. The obligation concerned moves to exception state.

The Rulebook must keep a clear audit trail of the disputed computation, supporting data, decision and resulting state.

IV.i Settlement-escrow availability of paying nodes

The paying node's operator ($RN > 0$), not Osnias, is responsible for keeping the corresponding settlement amount available, under its own control or through its authorised banking/custody provider.

Osnias has no unilateral power to move these funds. The Clearing Engine may record or receive proof that the settlement-escrow availability condition is met before releasing the corresponding settlement obligation.

For $RN > 0$: available settlement escrow $N \geq RN$

IV.j Inter-node settlement

On Monday, the first day of the next cycle (netting phase), escrow accounts are placed under the node manager's control. The manager first aligns its clients' escrows with the net dated statement using its manager key; that key

only allows movements between users of its own node, or to the node account for inter-node amounts. Nodes then align their positions with each other to balance out: an $RN > 0$ node pays, an $RN < 0$ node receives. Where applicable, each operator uses the available rail and the ISO 20022 profile it supports.

Osnias does not execute the transfer. It records the clearing obligation and may record the payment reference and the settlement status reported by the node operator or the external rail. All movements take place between user escrows and node accounts: none ever passes through an Osnias account.

Adjustment phase. On Tuesday in 1W, and from Tuesday to Thursday in 9W and 13W, the client regains control of its escrow account and freely changes the escrowed amount: it may adjust it, withdraw to its registered withdrawal address or top it up. The manager key has no effect on the escrow during this phase.

P2P period opens. At the start of the P2P period (Wednesday 00:00 in 1W; Friday 00:00 in 9W and 13W), the amount held in each escrow is booked as the opening net position of the cycle on the Sei ledger ($Pu(0) = Cu, \$4.q$), and P2P reopens. The escrowed amount then stays frozen for the whole cycle: no deposit or withdrawal is possible until the next adjustment phase.

Releasing final obligations at the end of the dispute window is not a universal guarantee of payment finality. The Time Oracle may shift the settlement date according to the business-day calendar and the availability rules of the settlement rail selected by the nodes concerned.

IV.k Internal allocation by the receiving node

A settlement-receiving node ($RN < 0$) performs its internal allocation/netting in favour of its end-users only after confirmation of actual receipt of the corresponding settlement funds.

$FundsReceivedN = TRUE \rightarrow ReceivingNodeInternalCompensationN = AUTHORIZED$

IV.l Network fees

Network fees are computed on the gross volume of position credits received by each end-user during cycle $N-1$ (sum of accepted receivables). They are not charged during the clearing freeze window of that same cycle.

$Feeu(N-1) = 0.0015 \times GrossVolumeReceivedu(N-1)$

The 0.15% fee is not a discretionary charge created by the smart contract. Its principle, calculation base and deferred P2P workflow are set out in the clearing agreement signed between the member and its local node. The smart-contract workflow technically executes a pre-existing contractual rule.

At the close of cycle $N-1$, the fee amount is crystallised into a fee obligation and communicated to the end-user through a separate invoice and the clearing statement. The participant thus has a documented basis to verify and, where appropriate, dispute the amount before any P2P fee order is submitted.

At the opening of cycle N , once P2P is reopened, the corresponding fee order is created from the end-user to the relevant node manager. The order then follows the ordinary P2P lifecycle and is included in the clearing of cycle N .

The node manager is treated as an ordinary clearing participant for balance computation and netting. The fee order therefore enters the same end-user computation, the same node aggregation and the same netting process as any other eligible P2P order.

For PFMI mapping and control purposes, fee collection confers no privileged accounting status on the node manager: its clearing position is included in the same node-level aggregations, reconciliations and audit checks as other end-user positions.

The fee invoice, fee obligation and P2P fee order MUST be linked by the cycle ID, the end-user's Osnias-ID, the node manager's Osnias-ID, the amount, the currency/unit, the calculation base and an immutable reference/hash.

Fee lifecycle: cycle N-1 activity → fee computation → invoice/notification → dispute → cycle N open → P2P fee order → cycle N clearing

ISO 20022 may be used for structured institutional notification, workflow status and reconciliation where the participant's environment supports it. The actual booking of fees on the position ledger remains an Osnias P2P order and is not executed by ISO 20022 itself.

IV.m Four distinct finality states

State	Meaning	Authority / evidence
Computation finality	End-user and node computations are final after dispute review.	Before release of settlement obligations.
Instruction irrevocability	Point beyond which the node/payment instruction can no longer be revoked under the applicable rail.	Defined by the external settlement rail / its Rulebook.
Settlement finality	The payment is final within the meaning of the applicable banking/payment system.	Confirmed by the external rail or the node operator.
Cycle finality	The Osnias cycle is closed and the relevant P2P state may reopen.	Once the required checks and settlement conditions are satisfied.

Acceptance of an ISO 20022 message does not equal settlement finality. A pacs.002 status, for example, must be interpreted under the Rulebook of the relevant settlement community and cannot be generically treated as proof of final settlement.

IV.n Exception handling and node default

The normal Monday sequence assumes that escrow alignment and inter-node balancing can be completed and evidenced within the day. If settlement is not final at the cycle deadline, the obligation concerned moves to exception state.

Exception	Fail-closed handling	Control principle
Settlement escrow unavailable at cut-off	The node's settlement instruction is not released.	The node remains restricted; another node's funds cannot cover the shortfall.
Payment rejected	Record the rejection and keep the obligation open.	The node operator must remediate through the applicable payment process.
Payment pending at deadline	Do not present the obligation as settled.	The node(s) concerned remain in exception state.
Material unresolved dispute	The settlement obligation concerned is not finalised.	Hold the instruction concerned until resolution.
Settlement finality not demonstrated	No internal allocation by the receiving node on the basis of expected funds alone.	Wait for final receipt/confirmation.

The Rulebook must specify whether only the node(s) concerned remain blocked in P2P or whether the whole network stays closed. Any selective reopening must be shown to be isolated, so that no unresolved obligation can contaminate the new cycle.

Exit from an exception state MUST be evidence-based, not discretionary. The affected perimeter may return to ELIGIBLE status only after reconciliation of the underlying discrepancy, validation and freshness of the relevant solvency or settlement proofs, and replay by the Clearing Engine of the corrected state using the same Cycle ID and audit references. A mere manual status change without supporting evidence is insufficient.

Any selective reopening MUST rest on objective isolation criteria defined in the Rulebook. The node concerned must be demonstrably isolated from any unresolved obligation, and the next cycle must neither import nor net an unresolved balance from the previous cycle.

IV.o Post-clearing mirror reconciliation

Once inter-node settlement and node-level internal netting steps are complete, the Clearing Engine MUST re-read the relevant EVM escrow states and the Sei clearing positions used for closing reconciliation.

$\text{EligibleEscrowEVM.post}(u) = \text{PositionSei.post}(u)$

Reconciliation is performed at end-user, node and clearing-chamber levels. Any material discrepancy puts the perimeter concerned into EXCEPTION state and prevents it from being presented as fully reconciled.

This closing mirror check is distinct from the real-time solvency monitoring and forms part of the cycle-finality evidence file.

IV.p On-ledger data and the purpose field

The canonical clearing ledger is maintained on Sei (Book 2) and accessed through dedicated RPCs, with no private blockchain network (Book 7). For each P2P order, only the parties' Osnias-IDs, the amount, the obligation references and the purpose field are written. Currency and cycle are not chosen order by order: they derive from the chamber, fixed at account opening as an invariant bound to the Osnias-ID (Book 1).

No name, address, identification number (SIREN, VAT number, LEI) or personal data is written on-chain. The mapping between Osnias-ID and legal identity is kept off-chain, in the database of the home node, which performs identity verification (KYC) before any account opening (Book 6). It is accessible only to the node concerned and to authorised authorities.

AML/CFT and travel rule. Each node applies customer due diligence obligations to its clients (know-your-customer, sanctions and politically exposed person screening). For any transfer between clients of different nodes, nodes exchange off-chain, over a secure channel, the originator and beneficiary information required by Regulation (EU) 2023/1113; the Osnias-ID routes this information without writing it on-chain.

R-PURPOSE rule. The purpose field is free-form by default. It is written in clear text and permanently on the canonical ledger. It MUST NOT contain any personal data or any nominative data identifying a natural or legal person (name, address, contact details, identification number, IBAN). The submitting participant is solely responsible for its content.

Mandatory warning. The submission interface MUST display, before any P2P order is validated, a warning stating that the purpose is public and permanent, and MUST require the user's explicit confirmation.

Node controls. The node MAY implement automated format checks (email addresses, IBANs, identification numbers) and reject an order whose purpose manifestly contains nominative data. Repeated breaches may be treated as a breach of protocol rules.

Hashed purpose option. To limit the risk of personal data being permanently written on-chain, the Rulebook MAY provide that the purpose is written on-chain only as a cryptographic hash, with the clear text kept off-chain by the nodes concerned.

This rule reconciles the traceability of the canonical ledger with the protection of participants' personal data and trade secrets.

IV.q Clearing position ledger and real-time solvency control

Major architectural simplification. As of Release 1.3, Osnias no longer issues a clearing token. Each member's clearing capacity is recorded natively as a position in the canonical Sei ledger. MINT and BURN operations, the

token contract and the associated issuance authority are removed. Solvency is no longer carried by an intermediate digital asset but by the ledger state itself.

Rationale for removing the clearing token. In earlier releases, the clearing token served as a security control: comparing the total locked in escrow on the EVM (Ethereum) side with the total tokens issued on the Sei side made it possible to verify that the clearing capacity in circulation remained strictly backed by escrowed funds. The introduction of the real-time solvency control, which directly compares the net total of positions on the Sei side, computed by the position oracle, with the total locked on the Ethereum side, computed by the escrow oracle and relayed through the Controllers, performs the same check without any intermediate object. The token therefore becomes redundant and adds nothing to security: it provides no additional guarantee, while requiring a token contract, MINT/BURN operations and an issuance authority that itself had to be secured. Removing it shrinks the attack surface and the complexity of the architecture without weakening the solvency control.

Qualification of positions. The absence of a token is not, by itself, enough to rule out a qualification under Regulation (EU) 2023/1114 (MiCA): the assessment turns on substance. The positions recorded on the Sei ledger nevertheless have features that argue against their qualification as crypto-assets: they are neither assignable nor negotiable; they cannot be moved outside the protocol; they change only through the booking of a commercial obligation accepted by the debtor; and they are extinguished at end-of-cycle netting. The final qualification rests with the competent authority (§2.f and §8).

Initialisation. At cycle open, for each member u :

$$Pu(0) = Cu$$

where Cu is the eligible principal actually locked in the member's EVM escrow and Pu its available clearing position on the Sei ledger. The escrowed amount is frozen for the whole cycle: it can only be changed during the adjustment phase of the closing period, when the client controls its escrow (§4.j).

State transition. Each accepted obligation updates the position directly:

$$Pu(t) = Cu + \text{accepted receivables} - \text{accepted payables}$$

Each accepted obligation of amount X books, within a single atomic transaction, $-X$ on the debtor's position and $+X$ on the creditor's. It therefore never changes the system total:

$$\sum_u Pu(t) = \sum_u Cu \quad \text{at every point in the cycle}$$

Example. A member locks €50,000: opening position 50,000. It accepts a €10,000 payable: 40,000. Another member acknowledges owing it €15,000: 55,000. New €20,000 payable: 35,000. This figure is its current state on the Sei ledger. At close, $\Delta u = 50,000 - 35,000 = 15,000$: the member is a net debtor of €15,000 (30,000 payable – 15,000 receivable).

Positive net position condition. A member's net position on Sei can never be zero or negative. A member can therefore only validate an ISO 20022 payment request, i.e. accept a payable of amount X , if its net position on Sei allows it. Before any debit write, the ledger contract enforces:

$$Pu(t) - X > 0$$

In integer monetary units of the chamber, this condition reads $Pu(t) - X \geq 1$ minimum unit (e.g. 1 euro cent): $Pu(t) > 0$ at all times. Otherwise, the ISO 20022 request cannot be validated: the write is rejected fail-closed and neither leg ($-X$, $+X$) is booked. The check, the debit and the credit execute in a single transaction, so that concurrent requests against the same debtor cannot jointly bring its position to zero or below.

Client exposure: debtor and creditor. As a debtor, the client is exposed to its own collateral only: it cannot commit beyond the amount it has placed in escrow, every obligation it accepts is covered by its escrow, which is frozen for the cycle, and the system grants no credit. As a creditor, however, the client bears the paying node's settlement risk during the Monday netting phase: between the pooling of inter-node amounts on the paying node's account and their receipt by the receiving node, a default or operational failure of the paying-node operator may

delay or compromise payment. The conservation invariant does not cover this risk, since escrows are moving during this phase. The Rulebook MUST provide measures to control this risk, for example atomic execution of inter-node settlement in a single multilateral transaction, a cap on each node's RN position, or a guarantee or dedicated own funds from the node operator. Losses are not mutualised between members.

Fee orders. The P2P fee order (§4.l) is written first at the opening of cycle N and is subject to the same check. If it is rejected, the fee obligation remains open and the member cannot write any new debit obligation until it is remediated, as specified in the Rulebook.

Real-time solvency control. The positive net position condition does not replace chamber-level monitoring. The chamber solvency control relies on two oracles: the escrow oracle, on the Ethereum side, reads the escrow contracts, totals them and relays the total to Sei through the Controllers; the position oracle, on the Sei side, reads each member's net balance and totals them. The control compares both totals, whose difference must be zero at all times:

$$TVL_EVM - Total_Sei = \sum u Cu - \sum u Pu(t) = 0$$

On the EVM side, the aggregate stays fixed for the whole cycle since escrows are frozen; on the Sei side, individual positions change continuously but their sum remains strictly identical. Any discrepancy immediately triggers FAIL status and halts new writes in the chamber (§7).

Three sources, one invariant. The EVM escrow shows how much has been locked; the Sei ledger shows how that capacity is distributed among members at time t; the obligation entry (references and purpose field, §4.p), portable to ISO 20022, shows which accepted obligation explains each change in that distribution. A member's position may rise or fall sharply, but the total mass is neither created nor destroyed during the cycle: this is conservation-based accounting, with no digital asset minted or burned.

IV.r Administration keys and powers

Principle. No entity has unilateral power of disposal over members' escrows. Each protocol key is described by its holder, scope and limits; the technical Rulebook keeps this register up to date and publishes any change.

- Client key: the only key able to withdraw to the registered withdrawal address or top up the escrow, during the adjustment phase.
- Node manager key: active only during the Monday netting phase; movements limited to the node's users and the node account; no withdrawal to an external address.
- Controllers: relay to Sei the escrow total computed by the escrow oracle; they can neither modify an escrow, nor book a position, nor move funds.
- Oracles (escrow, position, time): read and attest only; no power over funds.
- Contract upgrades (ledger, escrow, Controllers): MUST rely on a multisig arrangement of the governance entity and on a time lock announced in advance, allowing members to withdraw their escrow before it takes effect; an upgrade can under no circumstances transfer funds or change a balance.
- Emergency pause: limited to freezing new writes (fail-closed); it can neither move funds nor durably prevent withdrawals during the adjustment phase.

Osnias holds no key allowing it to withdraw, transfer or reassign escrowed funds. The actual holders of the multisig keys and the length of the time lock are specified in the technical Rulebook and Book 5.

IV.s Main risks

Without prejudice to the controls described, participants are exposed in particular to the following risks, which the Rulebook and client documentation MUST set out in a clear, fair and not misleading manner:

- Paying-node settlement risk during the netting phase (§4.q).
- Smart-contract risk: design or implementation flaws in the escrow, ledger or Controller contracts, despite audits.
- Oracle and Controller risk: unavailability, divergence or compromise of the cross-chain relay; the solvency control then switches to STALE or FAIL and halts writes.
- Settlement-asset risk: dependence on the issuer of EURC, an e-money token, and on its redemption regime.
- Infrastructure risk: unavailability, congestion, reorganisation or fork of the Ethereum or Sei networks.
- Node operational and cyber risk: compromise of a manager key, operating error.
- Legal risk: uncertainty over the regulatory qualification of the positions and of the arrangement (§2.f and §8).

V CYCLE CLOSING PERIOD: WHO DOES WHAT, WHEN

UTC	Actor	Action	Expected outcome
Friday 23:59:59	Time Oracle / position-ledger contract	Accept the last P2P order of the cycle.	End of the P2P activity period.
Saturday 00:00	Time Oracle / position-ledger contract	Close P2P until the end of the adjustment phase.	Clearing perimeter frozen.
Saturday 00:00	Clearing Engine	Read Sei RPC state and EVM escrow state; lock the snapshot.	Canonical dataset.
Saturday, before 06:00	Node operators	Compute Δu , publish each user's dated statement (PDF + structured record + hash) and send it to the client.	Each user receives verifiable evidence.
Saturday, before 06:00	Osnias – Clearing Engine	Compute RN, produce the consolidated dated node statement and send it to node managers.	Each manager receives its node's position.
Saturday–Sunday	Users / node managers	Review and dispute if needed (full freeze days).	Statements accepted or disputed.
Sunday 23:59	Clearing Engine / node operators	Close the window; resolve disputes; finalise Δu and RN; verify $\Sigma RN = 0$.	Final net dated statements.
Monday (day 1, netting)	Node manager	Using its manager key, align its clients' escrows with the net dated statement; movements limited to the node's users and the node account.	Escrows aligned; inter-node amount pooled on the node account.
Monday	Paying-node operator	For $RN > 0$, make $ RN $ available on the node account and provide proof.	Availability condition met.
Monday	Node operators	Balance nodes between node accounts ($RN > 0$ pays, $RN < 0$ receives); no movement to an Osnias account.	Nodes balanced.
Monday, after receipt	Receiving-node operator	Confirm receipt and credit its clients' escrows.	Internal allocations completed.

UTC	Actor	Action	Expected outcome
Monday, before 24:00	Clearing Engine	Mirror reconciliation; verify settlement proofs and exceptions.	Normal close or exception state.
Tuesday (1W); Tuesday–Thursday (9W, 13W)	Clients	Freely adjust one's escrow: withdrawal to the withdrawal address or top-up.	Final escrowed amount per client.
Wednesday 00:00 (1W); Friday 00:00 (9W, 13W)	Time Oracle / position-ledger contract	Freeze the escrowed amount and book it as the opening net position ($Pu(0) = Cu$); reopen P2P; write the validated fee orders of the completed cycle first.	The new cycle starts.

The following UTC sequence applies to the closing period, from Saturday 00:00 until the end of the adjustment phase (Tuesday 23:59 in 1W; Thursday 23:59 in 9W and 13W), at the end of the chamber cycle selected by the Time Oracle (1W, 9W or 13W). Outside this period, P2P remains governed by the Time Oracle according to the active cycle phase.

Closing calendar. The last P2P order of the cycle is accepted on the Friday of the final week at 23:59:59 UTC. P2P is closed from Saturday 00:00 until the end of the adjustment phase. Saturday and Sunday, two full freeze days, are dedicated to publishing dated statements and to disputes. Monday (netting phase): the node manager aligns its clients' escrows with the net dated statement, then nodes balance out with each other. The adjustment phase follows: on Tuesday in 1W, from Tuesday to Thursday in 9W and 13W, each client freely changes its escrow (withdrawal to its withdrawal address or top-up). At the start of the P2P period (Wednesday 00:00 UTC in 1W; Friday 00:00 UTC in 9W and 13W), the escrowed amount is booked as the opening net position on Sei; it stays frozen for the whole cycle.

V.a Chronological workflow

Osnias Clearing — Cycle closing period

P2P closed from Saturday 00:00 until the end of the adjustment phase · 1W / 9W / 13W profiles · Release 1.3 (position ledger, no token)



Figure — Osnias Clearing chronological workflow of the cycle closing period.

V.b Architecture and controls overview

Osnias Clearing — Architecture & controls · Release 1.3

Tokenless position ledger, time authority, ex-ante per-member solvency, real-time chamber oracle and sign convention

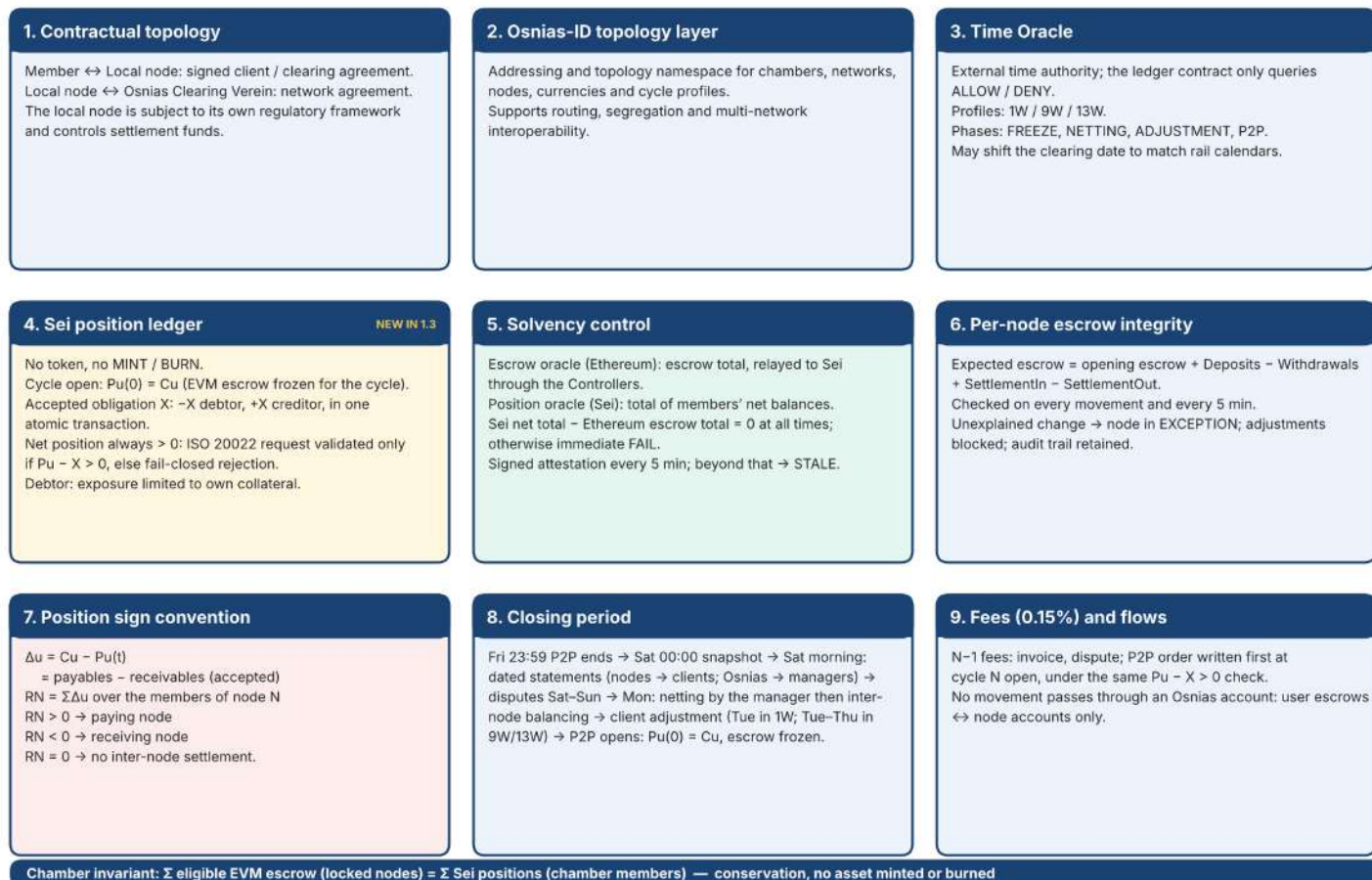


Figure — Osnias Clearing architecture and controls overview — Release 1.3.

VI REGULATORY AND TECHNICAL CONTROL MAPPING

Reference / topic	Regulatory issue	Osnias rule	Evidence / wording
PFMI 8	Settlement finality	Four-state finality model.	Separate timestamps/evidence for computation, irrevocability, settlement and cycle close.
PFMI 13	Default procedures	Fail-closed node exception.	Log of escrow unavailability / payment failures; no socialisation of the amount due.
PFMI 17	Operational resilience	Snapshot replayability and exception states.	Block hash, logs, deterministic computations.
PFMI 22	Recognised communications	Use ISO 20022 where the settlement rail supports it.	Message IDs linked to the Cycle ID.
FINMA perimeter	Payment-system qualification depends on functions and facts.	No self-qualification; functional separation explicitly documented.	Legal/regulatory analysis reserved.
Node sovereignty	Control over custody/payments must be clearly allocated.	The node operator controls accounts and settlement.	No disposal power for Osnias.
Accounting	Operational clearing $\neq$ automatic accounting offset.	Each participant is responsible for its accounting treatment.	No accounting conclusion is embedded in the Osnias output.

VI.a Audit file

- Cycle ID and UTC timestamps.
- Sei block height and block hash.
- End-user population and node attachment.
- Eligible EVM escrow principal and Sei position used for each Δu .
- Per-node escrow integrity check records: expected escrow, observed escrow, authorised adjustments/settlement, delta, status and timestamp.
- Log of net position checks ($P_u - X > 0$) and of ISO 20022 requests rejected fail-closed.
- ID of the generated PDF clearing statement and cryptographic hash.
- Proof that dated statements were published and sent on Saturday before 06:00 UTC (users by nodes, nodes by Osnias).
- Log of Monday movements signed with the manager key, showing that they remain limited to the node's users and the node account and that none passes through an Osnias account.
- Dispute log and evidence of resolution.
- Final RN per node and proof that $\sum RN = 0$.
- Trace of the paying node's internal allocation/netting.
- Proof of settlement-escrow availability under node control.

- Settlement obligation issued by Osnias.
- External payment instruction/reference and ISO 20022 identifiers, where applicable.
- Proof of settlement finality/receipt.
- Trace of the receiving node's internal allocation.
- Gross volume received and 0.15% fee computation.
- Cycle close or exception-state event.
- Cycle N-1 fee computation, separate invoice, dispute status, fee obligation ID and ID of the corresponding P2P order in cycle N.
- Proof that no P2P fee order was created during the frozen clearing window of cycle N-1.

Version history

Release 1.3 — 14 October 2026: major architectural simplification — clearing token and MINT/BURN operations removed; clearing positions are held natively in the canonical Sei ledger ($Pu(0) = Cu$; every accepted obligation books $-X$ on the debtor and $+X$ on the creditor); section 4.q added, including the rationale for removing the token (redundant with the solvency oracle); positive net position condition ($Pu - X > 0$: no ISO 20022 request validated without a sufficient net position on Sei; debtor client's exposure limited to its own collateral; fail-closed, atomic transaction); two-oracle solvency control (Ethereum escrow oracle, relayed to Sei through the Controllers, and Sei position oracle), in real time, with a signed attestation every five minutes; invariant Sei net total = Ethereum escrow total, zero difference at all times; closing calendar specified (P2P ends Friday 23:59; freeze and disputes on Saturday and Sunday; Monday netting by the node manager; client adjustment phase on Tuesday in 1W, Tuesday to Thursday in 9W and 13W; opening position and P2P reopening on Wednesday 00:00 in 1W, Friday 00:00 in 9W and 13W; escrow frozen during the cycle; no MINT/BURN operations); regulatory review: qualification of positions under MiCA, node licensing requirement, competent authorities in the EU and France, distinction between debtor exposure and creditor settlement risk, administration keys and powers (§4.r), main risks (§4.s), AML/CFT and the TFR, client categories, hashed purpose option.

Release 1.2 — 11 October 2026: cycle profiles aligned with Book 4 (Release 2.2): 1W (testnet), 9W (B2B commercial obligations) and 13W (eligible non-commercial obligations); section 4.p “On-ledger data and the purpose field” and rule R-PURPOSE added; Book 7 added to the corpus table; 24-hour clearing window aligned with the two-day end-of-cycle freeze and Monday settlement (Book 4).

Release 1.1 — 23 September 2026: exclusive MINT/BURN authority per node (KK, NNN), bounded by protocol controllers; node identity defined by the (KK, NNN) pair; legal-structure elements removed and referred to Book 5; Integrity & Conservation Oracle naming harmonised; Part III numbering corrected.

Release 1.0 — 23 September 2026: consolidation of clearing rules from drafts v5.x: sign convention ($RN > 0$ payer; $RN < 0$ receiver); 1:1 chamber-level conservation invariant; per-node escrow integrity check; 1W / 4W / 13W cycle profiles and 24-hour closing clearing window; settlement-escrow availability; deterministic EligibleEscrow definition; objective exception-exit criteria; contractual basis of the 0.15% fee.

VII CHAMBER INTEGRITY & CONSERVATION ORACLE AND PARTICIPANT TRANSPARENCY

VII.a Purpose and scope of the Chamber Integrity & Conservation Oracle

The Chamber Integrity & Conservation Oracle is a chamber-level observation and attestation layer. It does not determine the individual solvency of a node and does not require each node to show a zero clearing position during normal P2P activity. Positive and negative node positions are normal and are precisely what clearing operates on.

Two-oracle architecture. The chamber solvency control consists of two separate oracles. The escrow oracle, on the Ethereum side, reads the chamber's escrow contracts, computes their total and relays that total to Sei through the Controllers. The position oracle, on the Sei side, reads each member's net balance on the ledger and computes their total. The solvency control verifies that the Sei net total equals the Ethereum escrow total: the difference must be zero at all times.

Its purpose is to verify the conservation invariant of the chamber as a whole: the aggregate eligible escrow principal locked across all participating nodes must equal the aggregate clearing positions of all members of that same chamber.

The Integrity & Conservation Oracle has no custody function, no power to move funds and no time authority. Its two oracles read the states; the control computes the chamber-level invariant, timestamps the result and publishes an attestation. Time authority remains exclusively with the Time Oracle.

$\text{ChamberSolvency} = \text{EthereumEscrowTotal} \text{ (escrow oracle, via the Controllers)} - \text{SeiNetTotal} \text{ (position oracle)}$

Expected invariant: $\text{ChamberSolvency} = 0$ at all times

VII.b 1:1 chamber-level conservation invariant

For a chamber C comprising participating nodes N and admitted members u, the invariant is:

$$\sum N \text{ LockedEligibleEscrow} = \sum_{u \in C} \text{PositionSei}_u$$

This is a chamber-level conservation check. It must not be confused with $RN = \sum \Delta u$, which is the node's clearing position computed by the Clearing Engine. RN may be positive, negative or zero during the cycle, while the chamber's global solvency invariant remains exactly balanced.

Without a token, this invariant follows from the very construction of the ledger: every accepted obligation simultaneously books $-X$ on the debtor and $+X$ on the creditor, and, since escrows are frozen during the cycle, the sum of positions remains constant and equal to the aggregate escrow. A non-zero delta can therefore only result from an escrow change on the EVM side, which is prohibited during the cycle, or from ledger tampering on the Sei side; the oracle pinpoints its origin.

Buffers, reserves, fee balances or collateral amounts that are not part of the clearing principal must be accounted for separately and excluded from the eligible escrow value used in this invariant, in accordance with the technical Rulebook.

VII.c Real-time monitoring, five-minute attestation and freshness

The Chamber Integrity & Conservation Oracle runs this global check in real time: the escrow oracle recomputes the escrow total on every event affecting an escrow contract on the Ethereum side and relays it through the Controllers; the position oracle recomputes the net total on every new Sei block; both totals are compared continuously. Any non-zero delta immediately triggers FAIL status and halts new writes in the chamber (fail-closed). Independently of events, the oracle publishes a timestamped, signed attestation every five minutes, during normal operation and during the clearing window.

$t_0, t_0 + 5 \text{ min}, t_0 + 10 \text{ min}, \dots$

$$\text{Age}(\text{LastValidAttestation}) > 5 \text{ minutes} + \text{tolerance} \Rightarrow \text{STALE}$$

A stale attestation is never treated as a valid confirmation. The Rulebook defines the actions that require a current chamber solvency attestation in addition to the Time Oracle's time authorisation.

VII.d Interaction with the Time Oracle and the position-ledger contract

The Time Oracle and the Chamber Integrity & Conservation Oracle have distinct functions. The Time Oracle determines the current phase (FREEZE, NETTING, ADJUSTMENT, P2P) and whether the corresponding actions are OPEN/CLOSED under the selected 1W, 9W or 13W profile. The position-ledger contract queries the Time Oracle before execution; it does not embed the cycle calendar itself.

The Chamber Integrity & Conservation Oracle attests only the global 1:1 conservation state; the positive net position condition of each write is enforced by the ledger contract itself (§4.q). Where the Rulebook requires both conditions, execution is permitted only if the time authorisation and the required current solvency attestation are both valid.

$$\text{Time permission} = \text{Time Oracle state} \wedge \text{required chamber solvency condition}$$

VII.e Transparency on the end-user platform

The latest chamber solvency attestation must be visible read-only on the Osnias end-user platform. The display must show the chamber status, the time of the last check, the aggregate locked eligible escrow, the aggregate member positions, the chamber-level delta, the state/block references and the attestation ID.

The platform must not disclose other members' individual balances or positions. Transparency covers the chamber-level proof of conservation and its audit references.

Attestation field	Minimum content
Chamber ID	ID of the clearing chamber covered by the attestation.
UTC timestamp	Time of the oracle computation.
EVM state references	Block/state references used to aggregate the locked eligible escrow of participating nodes.
Sei state reference	Block/state reference used to aggregate the clearing positions of the chamber's members.
Aggregate locked eligible escrow	Total clearing principal included in the chamber-level check.
Aggregate member positions	Total clearing positions included in the same chamber perimeter.
Delta	ChamberSolvency.
Status	OK / WARNING / FAIL / STALE.
Attestation ID	Unique persisted/signed reference for audit and replay.
Node integrity check reference(s)	References to the separate per-node escrow integrity check records over the same observation window; these checks are not node solvency attestations.

VII.f Oracle failure model

Failure condition	Required behaviour
Escrow oracle (Ethereum) or Controllers unavailable	Do not issue a new positive attestation; keep the last one only as historical evidence and switch to STALE after the freshness threshold.
Position oracle (Sei) unavailable	Same fail-closed handling; do not assume conservation still holds.
Divergence between RPC/state sources	Do not publish OK until the reference state is deterministically resolved.
Inconsistent cross-chain references	Reject the attestation and recompute under the defined reference policy.
Non-zero chamber invariant	Publish FAIL for the chamber and apply the Rulebook controls that depend on the 1:1 conservation invariant.
Oracle process unavailable	Switch to STALE after the freshness threshold; never silently continue on a cached OK status.
Unexplained change in a node's escrow	Put the node concerned into EXCEPTION, block any new adjustment for that node, persist expected escrow, observed escrow and delta, then require reconciliation before returning to normal eligibility.

VII.g Audit and PoC test requirements

- The chamber invariant is validated when the aggregate locked eligible escrow exactly equals the aggregate member positions.
- An unauthorised withdrawal or unexplained change in a node's escrow is pinpointed by the integrity check, puts that node into EXCEPTION and blocks its adjustments even if the chamber aggregate remains balanced.

- Inter-node P2P activity may generate non-zero RN positions without causing a chamber solvency failure, as long as the chamber's global aggregate remains conserved.
- Any chamber-level aggregate discrepancy is detected and produces FAIL status.
- STALE status is produced when no valid attestation is available within the freshness window.
- The same defined EVM/Sei reference states reproduce the same chamber attestation result.
- The data displayed on the end-user platform matches the latest persisted/signed chamber attestation without exposing third parties' individual balances.
- A node operator cannot adjust any escrow attached to another (KK, NNN) pair, including where the same NNN exists on two different networks (e.g. node 01-042 on account 07-042); Osnias has no key allowing it to adjust an escrow.
- An ISO 20022 request such that $P_{debtor} - X \leq 0$ cannot be validated: the write is rejected and neither leg ($-X$, $+X$) is booked.
- Two concurrent requests against the same debtor cannot jointly bring its net position to zero or below (atomicity of the ledger transaction).
- No ledger-contract function can create or destroy a position other than through the opening entry $P_u(0) = C_u$ backed by a proven EVM state.
- Any attempt to deposit into or withdraw from an escrow during the P2P period is rejected.
- A delta artificially introduced between the EVM aggregate and the Sei aggregate produces FAIL status at the next block or event, without waiting for the five-minute attestation.

VII.h Updated control chain

Chamber Integrity & Conservation Oracle → Time Oracle authorisation → opening entry $P_u(0) = C_u$ → P2P writes under the positive net position condition (escrows frozen) → closing period → dated statements of users (nodes) and nodes (Osnias) → disputes → escrow alignment and inter-node balancing → post-clearing mirror reconciliation

This architecture preserves structural separation: the Time Oracle governs calendar permissions; the solvency control (Ethereum escrow oracle, Sei position oracle) attests chamber-wide 1:1 conservation; the Clearing Engine computes positions; node operators control the settlement escrow and execute settlement; Osnias does not hold settlement funds.

VIII Open points for legal counsel

- Enforceability of multilateral netting and node-level obligations in each relevant jurisdiction.
- Legal point of irrevocability and settlement finality for each external payment rail used by node operators.
- Legal nature of RN and of the settlement obligation generated from the finalised clearing result.
- Governing law, competent jurisdiction, default remedies and insolvency treatment under the Node Agreements and the Rulebook.
- Treatment of unresolved disputes, suspended nodes and selective reopening within the contractual framework.
- Accounting presentation of clearing positions, including the conditions for any accounting offset under the applicable framework.
- Legal and tax treatment of the 0.15% network fee invoice and its deferred P2P payment from cycle $N-1$ to cycle N .

- Qualification of the clearing positions recorded on the Sei ledger under MiCA, given that no token exists since Release 1.3: substance analysis (non-assignability, non-negotiability, extinction at netting, nature as a commercial claim); qualification and custody of the EURC locked on the EVM side. The preliminary analysis in Book 5 – Legal Qualification Memorandum must be updated accordingly.
- Application of Directive 98/26/EC on settlement finality and, where relevant, of the French Monetary and Financial Code to multilateral netting, transfer orders and the effects of insolvency proceedings.
- Impact of the federated contractual topology (end-user <-> local node <-> network governance entity, see Book 5) on the regulatory perimeter, any system designation, participant status or local licensing/supervision obligations.

IX Regulatory bibliography

Issuer	Reference	Official source
CPMI-IOSCO	Principles for Financial Market Infrastructures (PFMI)	https://www.bis.org/committees/cpmi/pfmi/overview
FINMA	Swiss financial market infrastructures / payment systems	https://www.finma.ch/en/authorisation/financial-market-infrastructures-and-foreign-market-participants/swiss-financial-market-infrastructures/
FINMA	Supervision of financial market infrastructures	https://www.finma.ch/en/supervision/financial-market-infrastructures/
ISO 20022	Message definitions — Payments Clearing and Settlement	https://www.iso20022.org/iso-20022-message-definitions
IFRS Foundation	IAS 32 — Financial Instruments: Presentation	https://www.ifrs.org/issued-standards/list-of-standards/ias-32-financial-instruments-presentation/
European Union	Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA)	https://eur-lex.europa.eu/eli/reg/2023/1114/oj
European Union	Directive 98/26/EC on settlement finality in payment and securities settlement systems	https://eur-lex.europa.eu/eli/dir/1998/26/oj
France — Légifrance	Monetary and Financial Code — provisions on payment/settlement systems and finality	https://www.legifrance.gouv.fr/codes/id/LEGITEXT000006072026/
AMF	Crypto-asset service providers (MiCA) — end of the PSAN transitional period	https://www.amf-france.org/fr/actualites-publications/actualites/lamf-rappelle-que-la-periode-transitoire-pour-les-psan-pour-continuer-de-fournir-des-services-sur
European Banking Authority	No Action Letter on the interplay between PSD2 and MiCA (e-money tokens)	https://www.eba.europa.eu/publications-and-media/press-releases/eba-publishes-no-action-letter-interplay-between-payment-services-directive-psd23-and-markets-crypto
European Union	Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets (TFR)	https://eur-lex.europa.eu/eli/reg/2023/1113/oj

Issuer	Reference	Official source
European Union	Directive (EU) 2015/2366 on payment services (PSD2)	https://eur-lex.europa.eu/eli/dir/2015/2366/oj

Technical and functional recommendation document. It does not constitute legal, regulatory, accounting or audit advice. Formal regulatory qualification, enforceability of netting/finality and obligations relating to settlement rails must be confirmed in the relevant jurisdiction and contractual framework.