SECURITY AUDIT READINESS &
INTERNAL TECHNICAL ASSESSMENT

PRE-AUDIT ÉDITION PAPER

Titile	SECURITY AUDIT READINESS & INTERNAL TECHNICAL ASSESSMENT
Author / Auteur ·	M.Denis Bouzon
ORCID	0009-0007-8894-8902
Release / date	1,0 ; septembre 14 th 2026
Landing page	www.osnias-clearing.com/security
Licence	Creative Commons Attribution 4.0 International (CC BY 4.0)
URL DOI	https://doi.org/10.5281/zenodo.22870678
URL HAL	https://hal.science/hal-05756811

Absract

This paper presents the Osnias Clearing end-user security architecture across the complete participant identity lifecycle: onboarding, dual-domain authorization, secure fund release, cryptographic renewal and off-boarding. Its objective is to reduce the risk that compromise of a single operational ECDSA key could result in diversion of escrowed funds.

The architecture uses existing chains as they are. It separates the operational EVM signing address, an independent Sei authorization domain, and a cold EVM release destination generated from a separate seed and pre-committed in the smart contract. The release destination is intended to remain non-signing during its designated receiving phase and to serve as a pre-committed beneficiary rather than an operational authorization key, so compromise of the operational signer does not, by itself, confer control over the destination of released funds.

A future Shor-enabled attack against exposed ECDSA public keys is treated as a prospective cryptographic risk, not as an asserted present operational threat. The design philosophy is long-horizon security engineering: use mechanisms available on current chains to reduce a plausible risk class extending across a long operational and cryptographic horizon, without claiming that ECDSA itself has become post-quantum secure. Document level: internal technical assessment and audit-readiness review. Controls are classified by evidence status; this document is not an independent audit, formal verification, penetration-test report or production-security certification.

Keywords

Osnias-ID ; onboarding ; off-boarding ; ECDSA ; secp256k1 ; EVM escrow ; quantum security ; cold release ; dual-domain authorization ; defence in depth ; cryptographic hygiene ; Shor-enabled attack ;

Résumé

Ce document présente l'architecture de sécurité end-user d'Osnias Clearing, organisée autour du cycle complet d'une identité participante : onboarding, autorisation dual-domain, libération sécurisée des fonds, renouvellement cryptographique et off-boarding. L'objectif est de réduire le risque qu'une compromission d'une seule clé opérationnelle ECDSA puisse entraîner un détournement des fonds séquestrés.

L'architecture conserve les chaînes actuelles telles qu'elles existent. Elle sépare l'adresse EVM opérationnelle utilisée pour signer, l'autorisation indépendante côté Sei, et une adresse EVM froide de destination des fonds, générée depuis une seed distincte et pré-engagée dans le smart contract. Cette adresse de release n'a pas vocation à signer pendant sa période de réception, de sorte que la compromission du signer opérationnel ne donne pas, à elle seule, le contrôle de la destination des fonds.

Le risque associé à une future attaque de type Shor contre des clés publiques ECDSA exposées est traité comme un risque prospectif et non comme une menace opérationnelle affirmée à ce jour. La philosophie de conception est celle d'une sécurité à long horizon : utiliser dès maintenant des mécanismes disponibles sur les chaînes actuelles pour réduire une classe de risque plausible sur un horizon opérationnel et cryptographique de long terme, sans prétendre rendre ECDSA post-quantique. Niveau documentaire : évaluation technique interne et préparation à l'audit. Les contrôles décrits sont classés selon leur niveau de preuve ; ils ne constituent pas une certification, un audit indépendant, une vérification formelle ou une qualification de sécurité en production.

Mots-clés :

Osnias-ID · onboarding · off-boarding · ECDSA · secp256k1 · escrow EVM · sécurité quantique · cold release · dual-domain authorization · défense en profondeur · cryptographic hygiene ; Shor-enabled attack

Table des matières

1. Assessment Status and Document Level

This document is an internal Security Audit Readiness & Technical Assessment of the intended Osnias Clearing end-user security design. It reviews architecture, trust boundaries, control objectives, open risks and the evidence required for later implementation validation. It does not represent an independent third-party audit, formal verification, penetration test, custody audit, legal opinion, certification or production-security approval.

Assessment item	Current status
Document level	Internal Security Audit Readiness & Technical Assessment
Review basis	Osnias Clearing End-User Security Architecture — Release 4.3
Reviewer	Denis Bouzon / Osnias Clearing — internal assessment
Implementation evidence	Pending for the controls identified in this document
Adversarial testnet campaign	Pending
Independent third-party audit	Not performed
Production-security certification	Not claimed
Overall status	Design assessed; implementation evidence, adversarial testing and independent review pending

Evidence-status vocabulary used in this assessment: DESIGN REQUIREMENT — intended security property; SPECIFIED — control semantics described; IMPLEMENTATION PENDING — code-level evidence not yet available; TESTING PENDING — adversarial evidence not yet available; OPEN — material design or implementation decision remains unresolved; INDEPENDENTLY REVIEWED — reserved for controls later examined by an identified independent reviewer.

2. Audit Scope, Methodology and Reference Frameworks

Assessment scope. The review covers the operational EVM signer, independent Sei authorization, pre-committed cold release beneficiary, composite release predicate, replay resistance, Osnias-ID and registry consistency, cross-chain verification assumptions, identity renewal and off-boarding, administrative control, participant key custody and the planned validation process.

Assessment exclusions. The review does not attest deployed bytecode, production infrastructure, wallet vendors, participant custody environments, source-chain consensus correctness, legal or regulatory compliance, or the effectiveness of controls that have not yet been implemented and evidenced. Although source-chain consensus correctness is outside the scope of this assessment, the cross-chain release design remains dependent on an explicitly documented finality and source-state-authentication assumption.

Methodology. Controls are assessed through architecture review, trust-boundary analysis, compromise-scenario analysis, invariant identification, lifecycle review, administrative-power analysis, cross-chain failure analysis, residual-risk identification and definition of implementation evidence and adversarial tests required before production qualification.

2,1 Reference frameworks used as methodological guidance

- ISO 19011:2026 — Guidelines for auditing management systems: audit principles, audit-program structure and evidence-based/risk-based audit practice.
- ISO/IEC 27001:2022 — Information security management systems: risk-governance and information-security management context.
- ISO/IEC 27002:2022 — Information security controls: control-oriented security guidance, including access control and cryptography-related practices.
- ISO/IEC 27005:2022 — Guidance on managing information security risks: structured risk identification, assessment and treatment.
- ISO/IEC 27034-1:2011 — Application security: integration of application security concepts and processes into the application lifecycle.
- NIST SP 800-218, SSDF v1.1 — Secure Software Development Framework: secure development practices, vulnerability reduction and evidence across the software lifecycle.

Reference-framework notice. These standards and frameworks are cited as methodological and security-design references only. Their citation does not imply ISO certification, conformity assessment, NIST endorsement, independent validation or a claim that Osnias Clearing has been audited against the complete requirements of any cited standard.

3. Control Assessment Matrix

The matrix below distinguishes design-level requirements from implementation evidence. Severity identifies the consequence of an absent or bypassed control; it is not a statement that a vulnerability has already been observed in deployed code. The Required next action column records the evidence or implementation work needed to advance each control toward verification.

ID	Control / finding	Severity	Current evidence status	Required next action
SEC-001	Operational signer must not select or substitute an arbitrary release beneficiary.	Critical	DESIGN REQUIREMENT	Implement and test contract-level beneficiary immutability / controlled-change logic; verify arbitrary-destination attempts fail closed.
SEC-002	Release authorization must be single-use and bound to nonce/proof identifiers and the committed beneficiary.	High	SPECIFIED	Implement nonce/proof consumption and test replay, cross-contract, cross-chain, amount and beneficiary substitution cases.
SEC-003	Canonical Sei-state authentication, finality/reorg policy, verifier quorum and verifier rotation require implementation evidence.	High	OPEN	Define the Sei state-authentication model, finality/reorg policy, verifier quorum and rotation procedure; implement failure and stale-state tests.

SEC-004	No single upgrade, registry, verifier or emergency authority should be able to bypass the composite release condition or rewrite the beneficiary unilaterally.	Critical	DESIGN REQUIREMENT	Define administrative role separation and threshold controls; test upgrade, registry, verifier and emergency-path abuse scenarios.
SEC-005	Seeds A, B and C require independent generation roots and common-mode isolation; participant custody controls are outside Osnias custody.	High	SPECIFIED / IMPLEMENTATION PENDING	Document key-generation and custody procedures; evidence independent roots/common-mode isolation and test onboarding misconfiguration cases.
SEC-006	Identity migration and successor binding require lifecycle-state enforcement and adversarial testing before verification.	High	IMPLEMENTATION PENDING	Implement lifecycle state machine, successor binding, migration gates and terminal revocation; execute adversarial migration tests.
SEC-007	Static analysis, testnet attack scenarios, remediation and retesting remain required before independent review.	High	TESTING PENDING	Run Slither and the planned adversarial testnet campaign; remediate findings, retest and publish the validation report.

Severity interpretation: Critical — absence could enable direct fund diversion or collapse of the intended authorization separation; High — material security control or trust-boundary weakness; Medium — weakness requiring correction before production; Low — hardening recommendation; Informational — observation without demonstrated direct security impact.

Administrative target invariant. No single upgrade, registry, verifier or emergency authority should be able to alter the release predicate, rewrite the registered release beneficiary or disable the independent second-domain condition unilaterally. The exact threshold, timelock and separation-of-duty mechanisms remain implementation evidence to be supplied before this control can be independently verified.

4. Purpose, Security Philosophy and Scope

Osnias Clearing treats end-user fund security as a lifecycle property rather than as a single-signature problem. The protocol separates operational signing, independent authorization, fund destination, registry state and identity lifecycle controls. The architecture is designed to be deployable on current EVM and Sei infrastructure while reducing the consequences of a future compromise of exposed classical signing keys.

Security design principle: do not require tomorrow's chains to reduce tomorrow's risk.

4.1 Long-horizon security perspective

Shor's algorithm establishes a theoretical path to solving the elliptic-curve discrete logarithm problem on a sufficiently capable quantum computer. This paper does not assert that such capability is presently available against secp256k1 accounts in operational blockchain conditions. The quantum scenario is therefore treated as prospective. The engineering question is narrower: if a future attacker recovers an exposed operational signing key, should that key alone be sufficient to divert escrowed funds?

Osnias answers this question architecturally. Rather than changing ECDSA, it changes the conditions under which funds can be released and where they can be sent. This is a defence-in-depth strategy, not a claim of post-quantum completeness.

4.2 What is claimed

- Compromise of the operational EVM signing key should remain insufficient, by itself, to satisfy the complete release predicate.

- A second independently generated authorization domain on Sei can add an independent cryptographic precondition.
- A pre-committed cold EVM release destination can separate signing authority from fund destination authority.
- The architecture can be implemented using existing EVM contracts, EOA addresses, registry state, nonces and authenticated cross-chain state.

4.3 What is not claimed

- No complete quantum resistance, formal reduction or quantified post-quantum security level is claimed.
- The cold release address does not make ECDSA post-quantum; it reduces the usefulness of compromise of the operational signer for fund diversion.
- Verifier, registry governance, source-chain consensus and upgrade authority remain explicit trust boundaries.

5. End-User Security Lifecycle

The end-user security lifecycle is organized as onboarding, active operation, secure fund release, optional identity renewal and off-boarding. Osnias provides the mechanisms and state transitions; the participant retains control over its own security policy, including whether and when to renew its cryptographic identity.

- Onboarding establishes the Osnias-ID and binds the operational EVM signer, the independent Sei authorization domain and the cold release destination.
- Active operation uses the operational signer for routine EVM interactions while the second domain and verifier constrain release authority.
- Fund release is directed only to the pre-committed release beneficiary, not to an arbitrary destination supplied at release time.
- Renewal and off-boarding create a new identity when desired, migrate or settle remaining positions, and end with irreversible revocation of the prior identity.

6. Secure Onboarding Architecture

Onboarding creates the security identity used by the protocol. Osnias-ID is the binding layer; it is not itself a cryptographic key. Security depends on separating the technical roles associated with that identifier.

6.1 Domain A — Operational EVM signer

Domain A contains the participant’s operational EVM signing key and address. Recommended end-user profile: the operational EVM key is generated and retained on a hardware wallet, so routine EVM signatures can be produced while private-key material remains isolated from the general-purpose host. This key is operational and potentially exposed through normal signing activity; it must not be the sole authority capable of determining the final destination of released escrow funds.

6.2 Domain B — Independent Sei authorization

Domain B is generated from an independent seed root and participates in the canonical Sei authorization or state-transition path. A participant may use an operational Sei-compatible wallet (for example, MetaMask where supported by the selected Sei environment) for routine Sei-side authorization. No shared seed, derivation root or recovery material should exist between Domain A and Domain B. Network separation alone is insufficient if the underlying seed material is common.

6.3 Domain C — Independent cold release destination

Onboarding also records a dedicated EVM release beneficiary generated from a third, independent seed. Recommended end-user profile: Seed C is retained offline as a cold release wallet and is normally unused for routine signing. Its address is registered as the release beneficiary. During its designated receiving phase it need not sign any transaction, so its public key is not revealed through an outgoing ECDSA signature merely by receiving funds.

The release beneficiary is pre-committed before the release event. The operational signer must not be able to substitute an arbitrary destination at release time. A change of release beneficiary should require a separately governed renewal or re-onboarding procedure rather than a unilateral action by the operational signer.

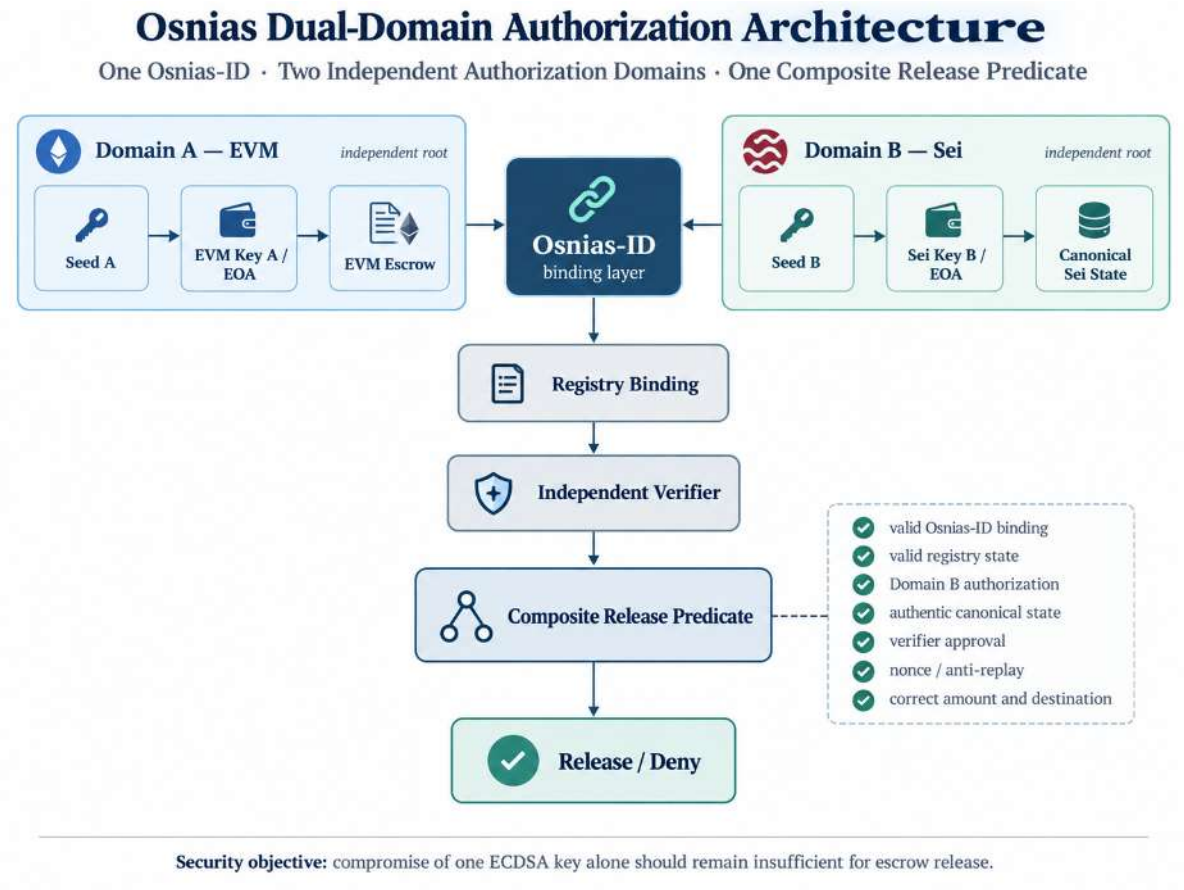

Figure 1 — Dual-domain authorization architecture

6.4 Seed independence and BIP-32 cascade risk

Seed A, Seed B and Seed C should be independently generated; shared roots undermine the intended separation. Multiple addresses derived from one common seed do not constitute independent security domains. Independent seed roots should also avoid a common compromised generation environment where practicable.

Participant custody responsibility. Seeds A, B and C, their private keys, recovery phrases, hardware devices and backup material remain under the end-user participant's custody and operational responsibility. Osnias Clearing does not hold, escrow, back up, recover or control participant private keys or seed phrases. The participant remains responsible for its key-generation environment, storage, recovery procedures, access controls and custody policy.

Common-mode isolation. Distinct seeds created on the same compromised device, session, recovery environment or shared administrative control plane do not provide complete fault-domain isolation. Institutional

deployments should evidence separation through controlled key ceremonies, segregated HSM/custody domains or equivalent approved procedures where appropriate.

Domain B signing risk. Independent authorization does not protect against malicious co-signing or blind signing. The target control is for Sei-side authorization to bind human-verifiable intent, Osnias-ID, beneficiary, asset, amount, nonce and expiry so the participant can verify what is being authorized before approval.

7. Composite Authorization and Secure Fund Release

The release function is designed around a composite predicate. A valid signature by the operational EVM signer is necessary only where the relevant protocol action requires it; it is not sufficient to redirect escrow funds.

7.1 Composite release predicate

Audit objective — composite release condition. The design requires a valid Osnias-ID binding, an acceptable registry state, authenticated second-domain authorization or canonical source-chain state, verifier approval, freshness and replay protection, and an exact match to the pre-committed release beneficiary. Contract-level enforcement remains subject to implementation evidence and testing.

If the composite predicate passes, funds are released to the registered cold beneficiary — never to a destination supplied ad hoc by the operational signer.

7.2 Pre-committed beneficiary rule

Design requirement — pre-committed beneficiary. The release beneficiary is intended to be committed during onboarding or an equivalently strong controlled process. The normal release path must not permit the operational signer to supply an arbitrary destination. Evidence of contract-level enforcement is required before this control can be marked as verified.

7.3 Minimum binding tuple

A production authorization should bind, at minimum: protocol version/domain separator; Osnias-ID; source and destination chain identifiers; verifying escrow contract; concrete asset identifier; ISO 4217 currency code where relevant; clearing cycle or mode; amount; unique nonce; canonical source-state reference; authorization or burn transaction identifier; release beneficiary commitment; timestamp; and expiry/freshness condition.

7.4 Single-use authorization and replay resistance

The proof must be single-use. The escrow should record consumption of the authorization nonce or proof identifier and reject replay, cross-contract substitution, cross-chain substitution, amount changes and beneficiary changes.

7.5 Release wallet lifecycle

The cold release address is non-signing during its designated receiving phase and is used as a pre-committed beneficiary, not as an operational authorization key. If the participant later moves those funds, the address enters an active signing phase. As an optional hygiene practice, the participant may then designate a newly generated cold release address for future releases. This remains a participant security-policy decision rather than a mandatory protocol interval.

8. Long-Horizon Threat Model: Single-Key and Shor Risk

Security goal SG-1 — Single-key insufficiency: recovery of one participant ECDSA private key, including the operational EVM signing key, must not by itself satisfy the complete authorization predicate for release of escrowed funds to an attacker-controlled destination. This is a target security property of the design, not an implementation finding or independently verified result.

8.1 Prospective Shor scenario

Shor's algorithm and its elliptic-curve adaptations make ECDLP polynomial-time on an ideal sufficiently capable quantum computer. The protocol does not change that fact. Instead, it assumes that a future attacker may obtain the operational private key corresponding to a public key exposed through normal signing activity and asks what the attacker can do next.

8.2 Attacker objective

The economically meaningful attacker objective is not merely to impersonate the signer. It is to cause the escrow to transfer legitimate participant funds to an attacker-controlled address. Release 4.3 separates these capabilities.

Compromise of 0xSIGNER does not imply control of 0xRELEASE.

8.3 Why the recovered signer remains insufficient

Recovery of the operational EVM key does not provide a known shortcut to the independently generated Sei key, does not create authentic canonical Sei state, does not satisfy the independent verifier, and does not reveal or control the private key of the independently generated cold release address. If the release beneficiary is immutable or strongly pre-committed, the attacker cannot simply substitute 0xATTACKER as the destination.

8.4 Residual attack surface

The attacker must therefore compromise or bypass additional trust boundaries: the second authorization domain, registry integrity, canonical-state verification, verifier control, upgrade governance or the release-beneficiary binding. These remain explicit residual risks.

9. Osnias-ID, Registry Integrity and Replay Protection

Osnias-ID binds the participant's security domains and lifecycle state. It does not create cryptographic strength by itself. Registry integrity is therefore a security boundary: bindings must be authentic, version-consistent and fail closed on divergence.

9.1 Registry consistency and TOCTOU

If an Osnias-ID binding can change after authorization is created but before EVM release, a time-of-check/time-of-use risk appears. Production logic should bind the authorization to a registry version, immutable release-beneficiary commitment or escrow-specific resolution state. Divergence between registry views should fail closed.

9.2 Control-plane separation

Upgrade, emergency and registry administration must not restore single-key release authority. In particular, the operational signer should not possess unilateral authority to rewrite the cold release destination or disable the second-domain requirement.

Verifier trust boundary. The cross-chain verifier is an explicit security boundary. Production implementation must define how canonical Sei state is authenticated, the accepted finality and reorganization policy, the mechanism for verifier rotation or replacement, and the quorum or proof condition required before an EVM release can proceed. Until evidenced in code and tests, SEC-003 remains OPEN.

10. WW=00: Standalone Escrow Security Mode

The same architecture can operate without clearing. WW=00 may be reserved as an explicit escrow-only mode: no clearing room, no 7/28/91-day cycle, no multilateral netting and no clearing-specific state transition. Osnias-ID then acts as the security binding between the EVM escrow, the independent authorization domain and the pre-committed release destination.

WW=00 means “no clearing cycle / escrow-only mode”. It must never be interpreted as a zero-week clearing cycle.

In this mode, the second-domain event need not be a burn. It may be a release authorization, mirrored state transition, policy approval or other uniquely bound event accepted by the verifier. The same single-key-insufficiency objective applies.

11. Cryptographic Hygiene, Identity Renewal and Off-Boarding

Osnias supports voluntary full renewal of a participant’s cryptographic identity as an operational-security and cryptographic-hygiene mechanism. The protocol does not prescribe a mandatory renewal interval. The participant decides whether and when to renew according to its own security policy, governance, custody arrangements and risk assessment.

A participant may choose annual, biennial, five-year, event-driven or other renewal cycles. These are participant decisions and do not represent a protocol-defined lifetime for ECDSA or secp256k1 keys.

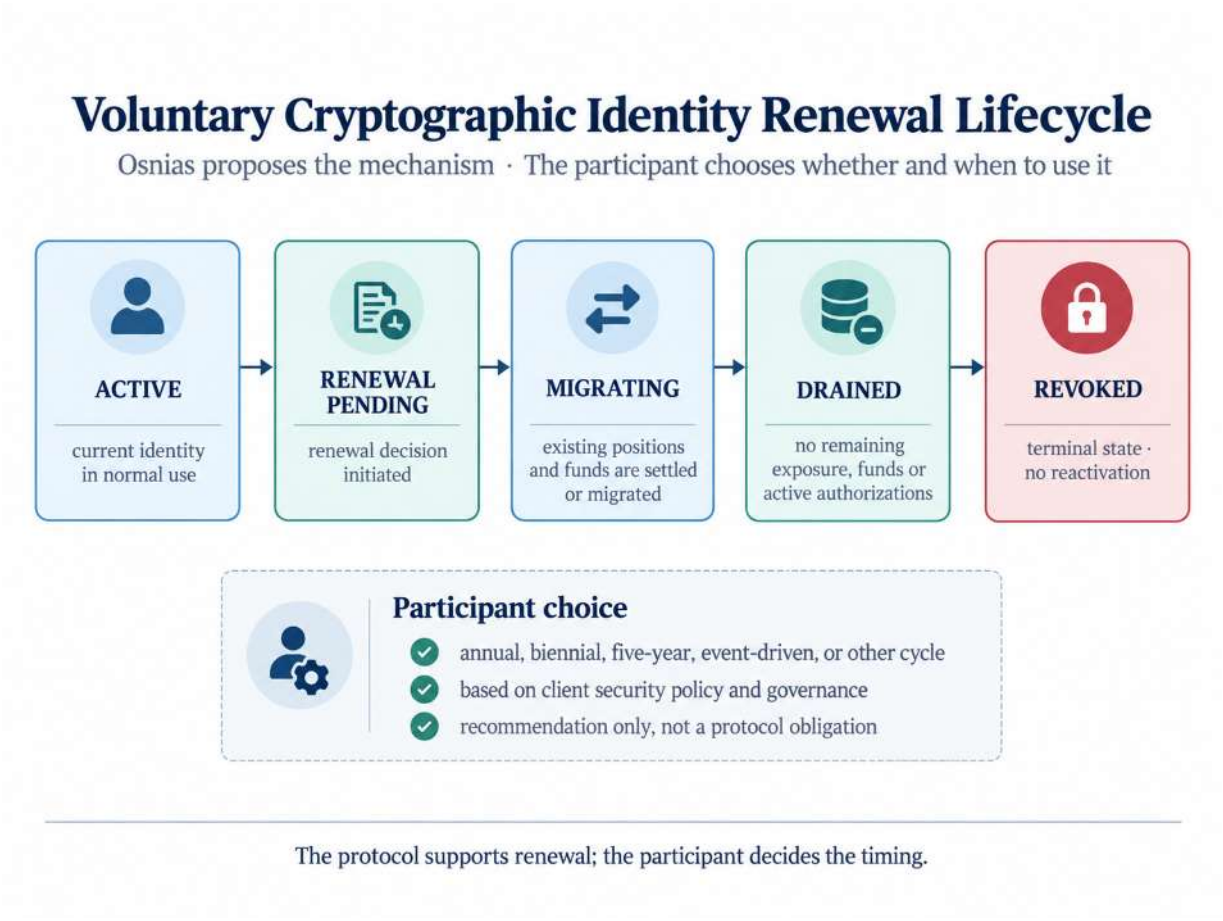

Figure 2 — Voluntary identity renewal lifecycle 10

11.1 Full renewal

A full renewal creates a genuinely new security identity rather than modifying an existing key binding in place. It may include a new Osnias-ID, a new independent EVM operational seed, a new independent Sei seed, a new independent cold release seed, new on-chain addresses, new registry bindings and controlled migration or settlement of existing positions and funds.

Migration risk boundary. Migration is treated as a heightened-risk lifecycle state. A successor binding should not become effective until migration authorization, registry version, destination commitments and remaining-position state have been verified. The implementation should prevent new exposure from being associated with the historical identity once the controlled transition is complete.

11.2 Off-boarding and terminal revocation

The previous identity remains available for historical verification and audit while losing all capacity to create new authorization events after final revocation. A possible lifecycle is ACTIVE → RENEWAL PENDING → MIGRATING → DRAINED → REVOKED. REVOKED is terminal and must not be reversible.

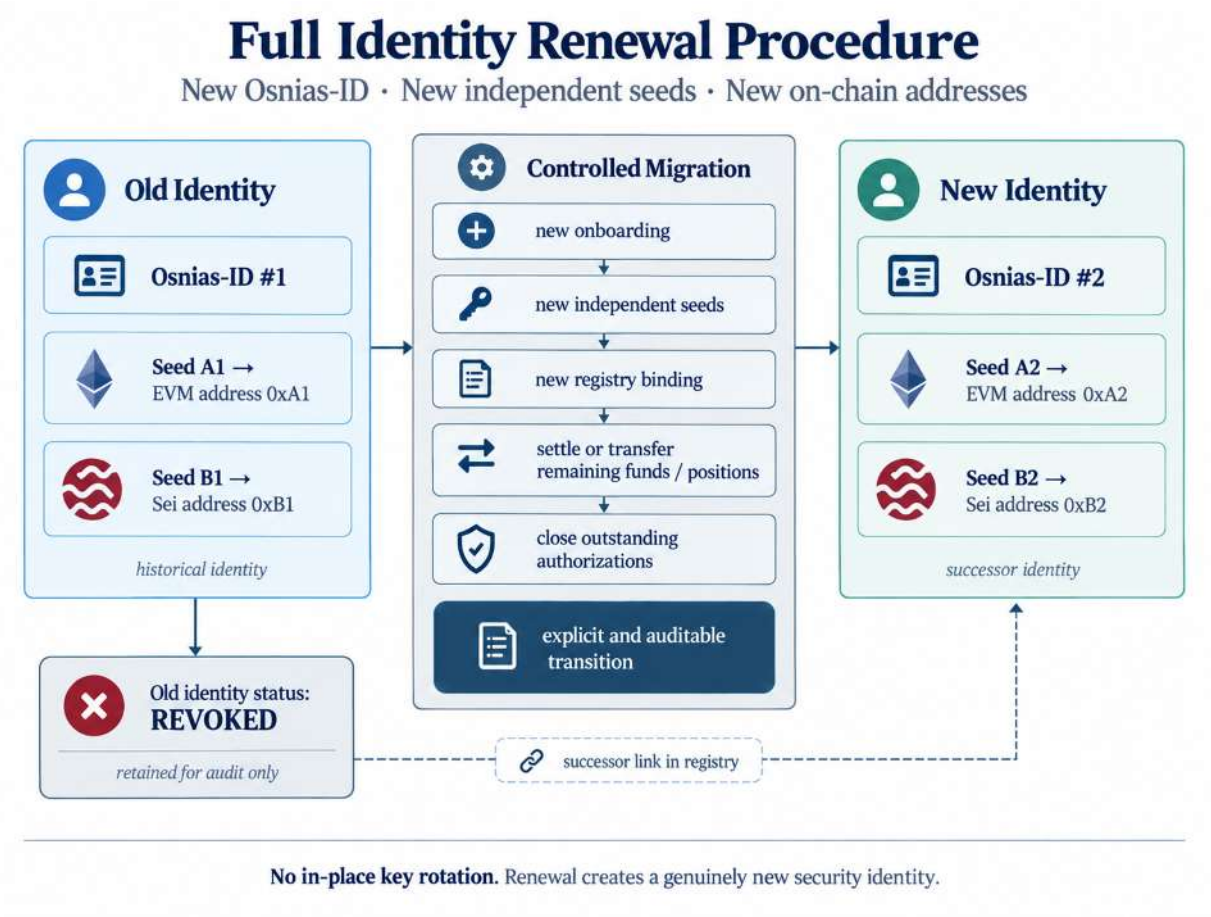

Figure 3 — Full identity renewal procedure 11

Where appropriate, the registry may retain a permanent successor reference from the revoked Osnias-ID to the new Osnias-ID without altering the historical key bindings of the previous identity.

12. Institutional Hardening Requirements

The architecture only survives production if operational controls preserve the separation assumed above. For institutional deployment, the following controls form part of the security model rather than administrative afterthoughts:

- independent key-generation domains and auditable key ceremonies, preferably with segregated HSM/custody domains;
- separate operator roles, backup and recovery paths, with explicit common-mode failure analysis;
- threshold or multi-party control for registries, verifier administration and emergency actions;
- defined key rotation, revocation, incident response and fail-closed procedures;
- immutable or tightly governed upgrade paths, with explicit separation of duties;
- no single upgrade authority may alter the release predicate or release beneficiary unilaterally;
- continuous audit logging and monitoring of registry, oracle/verifier and escrow state;
- crypto-agility so participant keys, registries and verifier authorities can migrate to standardized PQ or hybrid signatures without changing the semantic role of Osnias-ID.

Separate HSMs or approved random-generation processes provide operational evidence of key-domain separation; they do not mathematically prove independence of the complete system. Shared administrators, recovery material, vendor control planes or backup infrastructure can still create common-mode failure.

13. Limitations and Open Work

This paper intentionally stops short of a formal composition proof. Before any production security claim, the implementation should define a precise adversary and corruption model, the canonical-state verification mechanism, registry consistency semantics, verifier quorum and upgrade authority, release-beneficiary change policy, key-rotation behaviour, emergency procedures and a post-quantum migration strategy.

The result should be understood as defence in depth: it can increase adversarial work factor and attack preconditions, but it cannot transform classical ECDSA into a post-quantum signature scheme. Standardized post-quantum signatures address the primitive; Osnias addresses the composition question of whether one compromised operational key should be sufficient to exercise release authority or divert funds.

14. Implementation and Security Validation Roadmap

This assessment defines the intended Osnias Clearing end-user security architecture, threat model, trust boundaries, audit objectives and target security properties. It distinguishes design-level controls from evidence that must be produced by the implementation and validation process.

It does not claim that those properties have already been demonstrated by deployed production code, independently audited infrastructure or a certified operational environment.

The next stage is implementation of the described architecture on the Osnias public testnet, including the composite release predicate, registry bindings, independent authorization domains, pre-committed cold release destination, replay protection, lifecycle controls and fail-closed behaviour.

Once implemented, the deployed protocol will undergo a dedicated adversarial security campaign combining static analysis, integration testing and controlled attack scenarios against the implemented system.

The validation process is expected to include, where appropriate: static analysis of the deployed smart contracts, including Slither; adversarial testing of the release path and beneficiary binding; replay, substitution and stale-state tests; registry consistency and lifecycle-state tests; verifier and authorization-domain failure scenarios; upgrade, administrative and control-plane abuse scenarios; fail-closed behaviour under inconsistent or unavailable state; and remediation followed by retesting of identified findings.

The detailed attack methodology will be defined against the implemented system rather than fixed solely from the architectural design.

Following completion of the test campaign, Osnias intends to publish a separate Security Validation and Implementation Report.

That report should document the implementation actually tested, including relevant contract versions, deployment references, test conditions, executed attack scenarios, static-analysis findings, observed failures, remediation actions, retest results and residual risks.

This Audit Readiness assessment and the subsequent Security Validation and Implementation Report serve different purposes: this document defines the security design, control objectives, open findings and required evidence; the future report will document how the implemented protocol behaved under static analysis, adversarial testing, remediation and retesting.

No successful implementation or security outcome is assumed in advance.

15. Conclusion

Assessment conclusion. The reviewed design defines a meaningful separation between the operational EVM signer, the independent Sei authorization domain and the pre-committed cold release beneficiary. The principal security objective is narrow and testable: compromise of one operational ECDSA key should not, by itself, satisfy the complete release predicate or redirect escrowed funds to an attacker-controlled destination.

At the present document level, this remains a target security property and design objective, not an implementation finding or independently verified security result. Contract implementation, canonical-state authentication, verifier governance, administrative enforcement, adversarial testing, remediation and retesting remain necessary before the relevant controls can be treated as verified.

This document supports audit readiness and technical review. It does not constitute an independent third-party audit, formal verification, penetration-test report, certification or production-security qualification.

Designed for today’ s chains. Engineered one move ahead.

Bibliography

[1] P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” SIAM Journal on Computing, vol. 26, no. 5, 1997.

[2] J. Proos and C. Zalka, “Shor’s discrete logarithm quantum algorithm for elliptic curves,” Quantum Information & Computation, vol. 3, no. 4, 2003. arXiv: quant-ph/0301141.

[3] M. Roetteler, M. Naehrig, K. M. Svore, and K. Lauter, “Quantum resource estimates for computing elliptic curve discrete logarithms,” ASIACRYPT 2017, LNCS 10625.

[4] D. Johnson, A. Menezes, and S. Vanstone, “The elliptic curve digital signature algorithm (ECDSA),” International Journal of Information Security, 2001.

[5] SECG, SEC 2: Recommended Elliptic Curve Domain Parameters, Version 2.0, 2010.

[6] NIST, Module-Lattice-Based Digital Signature Standard, FIPS 204, 2024.

[7] NIST, Stateless Hash-Based Digital Signature Standard, FIPS 205, 2024.

[8] NIST SP 800-90A Rev. 1 and SP 800-90B, random bit generation and entropy-source recommendations.

[9] P. Wuille, BIP-32: Hierarchical Deterministic Wallets, 2012.

[10] G. Wood, Ethereum: A Secure Decentralised Generalised Transaction Ledger (Ethereum Yellow Paper).

[11] Sei Labs, Sei technical documentation, consensus and EVM documentation.

[12] D. Bouzon, “Osnias-ID: An internal interchain identifier for multi-chain clearing,” Osnias Clearing Technical Report, Release 2.0, 2026.

[13] ISO 19011:2026, Guidelines for auditing management systems, Edition 4, May 2026.

[14] ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection — Information security management systems — Requirements.

[15] ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection — Information security controls.

[16] ISO/IEC 27005:2022, Information security, cybersecurity and privacy protection — Guidance on managing information security risks.

[17] ISO/IEC 27034-1:2011, Information technology — Security techniques — Application security — Part 1: Overview and concepts (confirmed current by ISO review).

[18] NIST Special Publication 800-218, Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities, 2022.

Standards-reference notice: references [13]–[18] are methodological and security-design references. Their citation does not imply certification, conformity assessment, endorsement or independent validation of Osnias Clearing.

