LIVRE 6

Onboarding des clients sur un nœud

Titre	**LIVRE 6 : Onboarding des clients sur un nœud**
Auteur ·	**M. Denis Bouzon**
ORCID	**0009-0007-8894-8902**
Version / date	**1,0 ; 28 septembre 2026**
Page de présentation	**www.osnias-clearing.com/onboarding/**
Licence	**@Copyright Osnias-clearing** **Creative Commons Attribution 4.0 International**
URL DOI	**https://zenodo.org/uploads/23010805**

Résumé

Le Livre 6 décrit le parcours opérationnel par lequel une entreprise devient participante d'un nœud Osnias Clearing, alimente un séquestre en EURC natifs sur Ethereum et accède au clearing canonique sur Sei. Il transforme les principes d'identité, d'architecture, de clearing, de synchronisation et de sécurité définis par les Livres précédents en une procédure cohérente d'admission, d'activation et de sortie.

Mots clef

Onboarding ; gestionnaire de nœud ; EURC ; USDC ; Ethereum ; Sei ; séquestre ; Osnias-ID ; KYB ; AML ; SEPA ; self-custody ; netting.

Conclusion structurante

Le nœud prend en charge l'admission, la passerelle SEPA et la conversion EUR vers EURC puis EURC vers EUR. Le participant conserve seul ses trois graines indépendantes. La libération du séquestre ne peut pas être redirigée par la seule clé EVM opérationnelle : elle aboutit au bénéficiaire EVM froid prédéfini.

Table des matières

1 Position dans le corpus documentaire et statut

Le Livre 6 est un document autonome dans la continuité logique du corpus Osnias Clearing. Il décrit comment les principes définis par les Livres 1 à 5 deviennent un parcours client exploitable par le participant et son gestionnaire de nœud. Il ne remplace aucune règle antérieure : il les assemble au point d'entrée opérationnel, depuis l'admission jusqu'à l'offboarding.

Document	Fonction	Apport au parcours
Livre 1	Osnias-ID	Identité du participant et liens entre chaînes.
Livre 2	Architecture	Séparation du clearing, du règlement et du collatéral.
Livre 3	Règles de clearing	Obligations, netting, gouvernance et responsabilités.
Livre 4	Cycles et calendrier	Synchronisation temporelle et états des opérations.
Livre 5	Sécurité	Domaines A B C, condition composite et modèle de menace.
Livre 6	Onboarding	Admission, passerelle EUR EURC, séquestre et sortie.

Statut documentaire Il s'agit d'une architecture fonctionnelle et d'exigences de conception. Le document ne constitue ni un audit indépendant, ni une vérification formelle, ni un test d'intrusion, ni une certification de sécurité ou une autorisation de mise en production.

2 Décisions d'architecture

Principe	Application
Responsabilité du nœud	Le nœud organise le KYB et l'AML, vérifie le compte bancaire, fournit la passerelle EUR et EURC et assume le parcours d'entrée comme de sortie.
Conservation par le participant	Les graines, clés privées, phrases de récupération, appareils et sauvegardes restent sous la garde exclusive du participant.
Trois domaines indépendants	A est le signataire EVM opérationnel, B l'autorisation Sei indépendante et C le bénéficiaire EVM froid prédéfini.
Ethereum natif	Le collatéral admis dans ce parcours est l'EURC natif Ethereum, sans bridge, wrapper ni représentation synthétique.
Sei canonique	Sei porte l'état canonique du clearing et le calcul du netting. Ethereum verrouille le collatéral et applique un résultat authentifié.
Osnias non-custodial	Osnias Clearing ne reçoit ni euros, ni EURC, ni clé privée. Il fournit les règles, les registres et le calcul des positions.

Principe	Application
EOA-only	Les adresses liées à l'Osnias-ID sont des comptes externes vérifiés. Aucun smart account tiers ne constitue l'identité du participant.

2.1 Pourquoi Ethereum comme couche native de séquestre

Ethereum est retenu comme réseau EVM natif de séquestre et de collatéral pour sa décentralisation, sa neutralité structurelle et la maturité de son environnement de sécurité. Il accueille nativement l'USDC et l'EURC et concentre une profondeur monétaire adaptée aux besoins institutionnels. Le gestionnaire de nœud ou son partenaire régulé peut ainsi organiser les passerelles EUR et EURC ainsi que USD et USDC sans bridge, wrapper ni représentation synthétique.

Le choix tient également à l'absence d'un opérateur unique contrôlant la chaîne de base. Cette propriété réduit la dépendance du séquestre à une entreprise particulière et renforce la continuité attendue pour un collatéral destiné à garantir des obligations de clearing entre plusieurs juridictions.

Comparaison des réseaux Au 28 septembre 2026, Circle Mint prend en charge l'USDC mais pas l'EURC sur Arbitrum. Arbitrum ne fournit donc pas la passerelle directe EUR et EURC recherchée. Base et Avalanche prennent en charge les deux actifs, mais présentent une empreinte institutionnelle plus concentrée : Base est développée par Coinbase, tandis qu'Avalanche demeure étroitement associée à Ava Labs et à l'Avalanche Foundation. Ces réseaux restent techniquement utilisables, mais offrent une neutralité structurelle moindre pour le rôle de séquestre de référence.

Coût des transactions Les frais d'Ethereum peuvent être supérieurs à ceux des réseaux de couche 2 ou d'autres EVM. Ce paramètre n'est toutefois pas prépondérant dans l'architecture Osnias : Ethereum n'exécute ni les paiements courants, ni le calcul des positions, ni le netting. Il reçoit un nombre limité d'opérations de collatéral, principalement le dépôt, le gel éventuel, la libération et la sortie. Le volume opérationnel reste porté par Sei. Le coût Ethereum est donc supporté par quelques transitions de séquestre, et non par chaque opération intégrée au clearing.

3 Acteurs et responsabilités

Acteur	Responsabilité principale
Participant	Génère et conserve les domaines A, B et C, vérifie les intentions de signature, finance le séquestre et décide de son renouvellement cryptographique.
Gestionnaire de nœud	Admet le participant, réalise les contrôles KYB et AML, vérifie son compte bancaire, assure ou fait assurer la conversion EUR et EURC et administre la relation client.
Osnias Clearing	Définit les règles, coordonne les cycles, maintient les fonctions du registre et calcule les positions sans détenir les actifs ou les clés du participant.
Séquestre Ethereum	Reçoit les EURC natifs, applique les états du cycle, contrôle la condition composite et ne libère les fonds qu'au bénéficiaire C enregistré.
Registre Sei	Conserve l'état canonique du clearing, l'autorisation indépendante et les positions individuelles et agrégées utilisées pour le netting.
Vérificateur	Authentifie l'état Sei présenté au contrat Ethereum selon une politique de finalité, de fraîcheur, de quorum et de rotation qui reste une frontière de confiance.
Partenaire régulé	Fournit au nœud, lorsque nécessaire, l'accès institutionnel à l'émission ou au remboursement de l'EURC. Le nœud reste responsable de la prestation fournie au participant.

4 Frontière de conservation

Le gestionnaire de nœud vérifie des adresses, des signatures et des états ; il ne reçoit jamais les secrets permettant de les produire. Osnias Clearing ne détient, ne séquestre, ne sauvegarde, ne récupère et ne contrôle aucune clé privée ou phrase de récupération. Le caractère non-custodial d'Osnias n'efface pas les obligations réglementaires propres au nœud ou à son partenaire lors des conversions fiat.

5 Identité de sécurité créée à l'entrée

Domaine	Fonction	Exigence
A	Signataire EVM opérationnel	EOA Ethereum utilisée pour les dépôts et les interactions courantes. Portefeuille matériel recommandé. Cette clé ne choisit jamais seule la destination d'une libération.
B	Autorisation Sei indépendante	Adresse issue d'une graine distincte. Elle autorise une intention ou une transition canonique liée à l'Osnias-ID, au montant, au bénéficiaire, au nonce et à l'expiration.
C	Bénéficiaire EVM froid	EOA Ethereum issue d'une troisième graine, enregistrée avant la libération. Elle reçoit les fonds mais ne signe pas pendant sa phase froide de réception.

5.1 Indépendance des graines

Les domaines A, B et C doivent provenir de racines indépendantes. Trois adresses dérivées d'une même graine BIP-32 ne constituent pas trois domaines de sécurité. Aucune phrase de récupération, racine de dérivation ou sauvegarde commune ne doit être utilisée. Dans un déploiement institutionnel, la séparation peut être étayée par des cérémonies de création, des HSM ou des domaines de conservation distincts.

Adresse C La procédure d'onboarding ne doit pas obliger l'adresse froide C à signer une opération courante. Le participant transmet son adresse publique et confirme sa procédure de sauvegarde selon les contrôles du nœud ; la clé privée et la phrase de récupération restent hors ligne.

5.2 Association par Osnias-ID

Osnias-ID relie l'entreprise admise, son nœud, les domaines A, B et C, la devise et le profil de cycle. Il ne constitue pas une clé cryptographique. Les associations doivent être cohérentes entre les registres et toute divergence doit bloquer l'activation ou la libération.

6 Parcours d'onboarding

Le parcours relie la passerelle fiat du nœud, les trois domaines indépendants du participant et les deux registres on-chain. Le flux supérieur représente l'entrée en EURC et le dépôt ; le flux central porte l'autorisation canonique ; le flux inférieur représente la libération sécurisée et le remboursement.

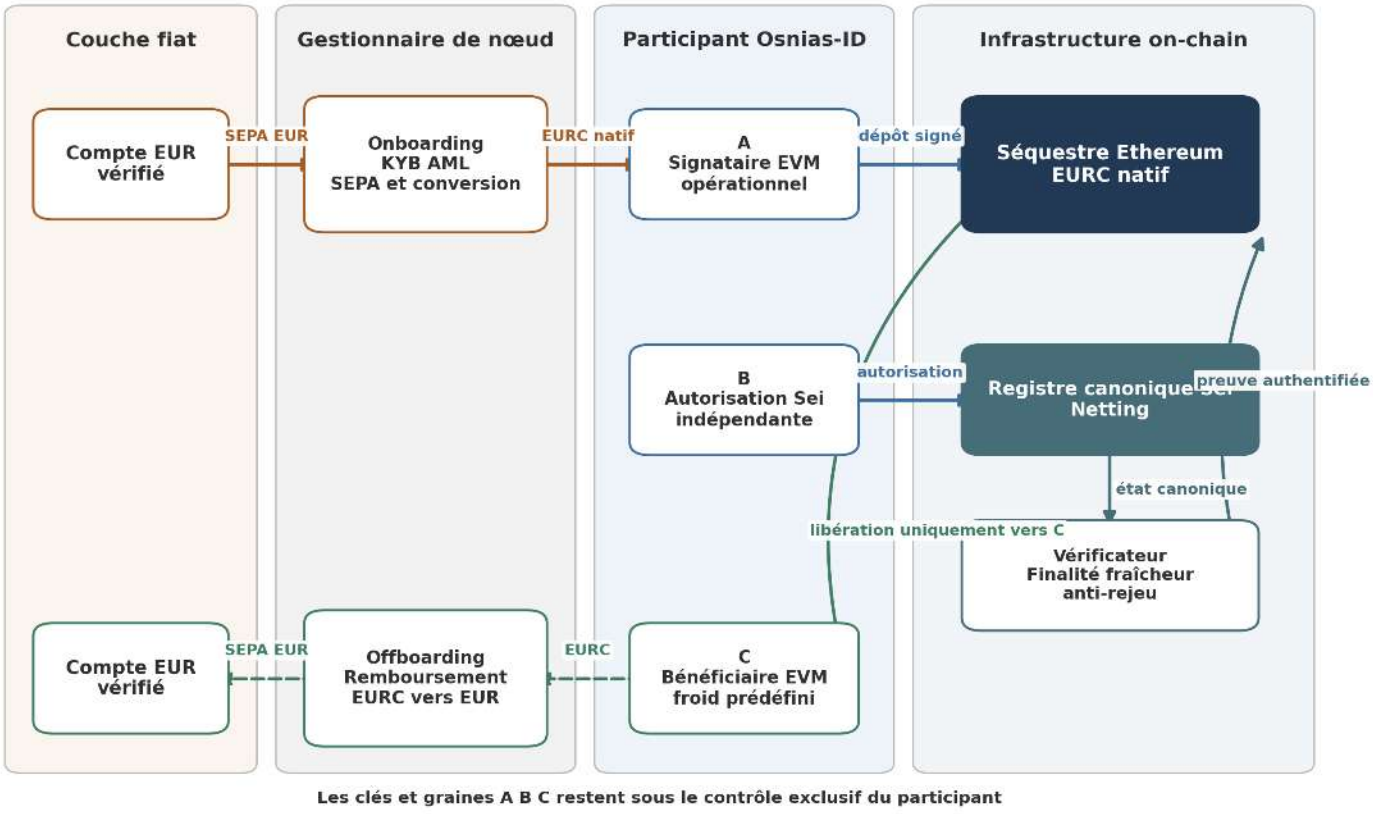

Figure 1 Parcours d'onboarding et condition de libération

6.1 Séquence opérationnelle

Étape	Phase	Résultat attendu
1	Admission	Le nœud identifie l'entreprise, ses représentants et bénéficiaires effectifs, vérifie le compte bancaire et applique ses procédures KYB et AML.
2	Création des domaines	Le participant génère séparément A, B et C dans des environnements appropriés et conserve seul les secrets et sauvegardes.
3	Preuves et enregistrement	A et B prouvent leur maîtrise par des challenges à domaine explicite, nonce unique et expiration. C est enregistré comme bénéficiaire froid sans être utilisé comme signataire courant.
4	Osnias-ID	Le nœud associe l'identité admise, son propre identifiant, les trois domaines, la devise et le profil de cycle dans les registres autorisés.
5	Conversion EUR EURC	Le participant vire les euros par SEPA. Le nœud réalise ou fait réaliser la conversion et livre les EURC natifs Ethereum à l'adresse A vérifiée.
6	Dépôt Ethereum	Le participant autorise puis signe le dépôt des EURC dans le contrat de séquestre lié à son Osnias-ID et à son nœud.
7	Activation	Le système contrôle le token officiel, les associations, le bénéficiaire C, l'état du cycle, le montant finalisé et l'absence de divergence entre registres.

6.2 Conditions minimales d'activation

- KYB et contrôles AML validés par le nœud ;
- compte bancaire au nom du participant vérifié ;
- Osnias-ID actif et rattaché au bon nœud, à la bonne devise et au bon profil de cycle ;
- domaines A, B et C enregistrés avec des racines déclarées indépendantes ;
- adresse C fixée comme bénéficiaire de libération avant l'exposition au clearing ;
- EURC natifs Ethereum déposés et transaction finalisée ;
- capacité de clearing limitée au collatéral reconnu comme éligible ;
- contrôle fail-closed en cas d'état incohérent, incomplet ou périmé.

7 Séquestre Ethereum et condition de libération

Le contrat de séquestre relie techniquement le participant à son gestionnaire de nœud sans donner à ce dernier un pouvoir discrétionnaire de retrait. Il verrouille les EURC natifs, publie les événements utiles à la preuve de solvabilité et applique les transitions permises par le cycle. Son application effective reste à démontrer par le code et les tests.

7.1 Données liées à une autorisation

Catégorie	Contenu minimal
Domaine	Version du protocole, séparateur de domaine, Osnias-ID et identifiants des chaînes source et destination.
Contrats	Adresse du séquestre, adresse du vérificateur et adresse officielle de l'EURC natif Ethereum.
Opération	Code devise, cycle ou mode, montant, nonce unique, horodatage et condition d'expiration.
État canonique	Référence de l'état Sei, identifiant de l'autorisation ou de l'opération et niveau de finalité requis.
Destination	Engagement exact du bénéficiaire C préalablement enregistré.

7.2 Condition composite

- Osnias-ID valide et associations cohérentes dans leur version applicable ;
- état du cycle autorisant la libération et absence d'obligation active ou contestée ;
- autorisation B ou état canonique Sei authentifié par le vérificateur ;
- finalité, fraîcheur, quorum et politique de réorganisation satisfaits ;
- nonce ou preuve non encore consommé et correspondance exacte du montant, de l'actif et des contrats ;
- destination strictement égale au bénéficiaire froid C enregistré.

Invariant de destination La compromission de la clé A ne doit pas permettre de remplacer C par une adresse choisie au moment de la libération. Aucune voie administrative unique ne doit pouvoir contourner cette condition.

8 Netting et articulation avec Sei

Le séquestre Ethereum ne calcule pas le netting. Les positions individuelles sont calculées et consolidées sur Sei, puis agrégées par nœud afin de déterminer les obligations nettes et le résidu inter-nœuds. Ethereum reçoit uniquement le résultat canonique nécessaire au gel, au règlement ou à la libération du collatéral.

- la somme des positions du cycle demeure égale à zéro ;
- la capacité de clearing ne dépasse pas le collatéral EURC reconnu comme éligible ;
- le résultat individuel se réconcilie avec l'agrégation du nœud ;
- le miroir post-clearing rapproche l'état canonique Sei et l'état final du séquestre Ethereum ;
- seul le résidu après compensation interne du nœud est exposé au règlement inter-nœuds ;
- tout écart entre les registres bloque les nouvelles opérations jusqu'à réconciliation.

9 Offboarding burn et libération du collateral, vers compte bancaire

1. Le participant demande sa sortie depuis le domaine A enregistré.
2. Le système vérifie qu'aucun montant n'est gelé, contesté ou affecté à une obligation active.
3. La condition composite est vérifiée, y compris l'autorisation B ou l'état Sei authentifié et la protection contre le rejeu.
4. Le contrat libère exclusivement les EURC vers l'adresse froide C prédéfinie.
5. Le participant transfère ensuite les EURC depuis C vers l'adresse de remboursement communiquée par le nœud.
6. Le nœud réalise ou fait réaliser la conversion EURC vers EUR et vire les euros vers le compte bancaire vérifié.
7. Après règlement des positions restantes, l'identité passe à l'état SOLDÉ puis RÉVOQUÉ de manière irréversible.

Conséquence de l'utilisation de C Dès que l'adresse C signe pour transférer les fonds reçus, elle quitte sa phase froide. En cas de maintien dans le dispositif après une libération partielle, un nouveau bénéficiaire froid doit être enregistré par une procédure de renouvellement protégée.

10 États de l’identité et du séquestre

Objet	État	Effet
Identité	PRÉINSCRIT	Admission en cours ; aucune capacité de clearing.
Identité	ACTIF	Associations A B C validées et exposition autorisée dans les limites du collatéral.
Identité	RENOUVELLEMENT EN ATTENTE	Nouvelle identité préparée ; l’ancienne ne peut accroître son exposition.
Identité	MIGRATION	Positions et fonds sont transférés ou réglés sous contrôle renforcé.
Identité	SOLDÉ	Aucune position ni obligation ne subsiste.
Identité	RÉVOQUÉ	État final irréversible ; historique conservé pour audit.
Séquestre	FUNDED ELIGIBLE	EURC finalisés et montant reconnu comme capacité potentielle.
Séquestre	FROZEN CONTESTED	Montant indisponible pendant le calcul ou la contestation.
Séquestre	CLEARED RELEASABLE	Résultat authentifié ; montant libérable uniquement vers C.

11 Contrôles et risques à traiter

Risque	Traitement attendu
Racine commune	Une graine BIP-32 commune annule la séparation A B C. Contrôle de procédure et preuves institutionnelles attendus.
Signature aveugle B	L'intention affichée doit lier Osnias-ID, actif, montant, bénéficiaire, nonce et expiration dans un format lisible.
Substitution de C	Le contrat rejette toute destination différente du bénéficiaire enregistré et encadre séparément son renouvellement.
Rejeu ou substitution	La preuve est à usage unique et liée à la chaîne, au contrat, au cycle, au montant et au bénéficiaire.
Divergence TOCTOU	Une version de registre ou un engagement immuable est fixé ; toute divergence entre contrôle et exécution bloque l'opération.
Vérificateur	Authentification, finalité, réorganisations, quorum, rotation et états périmés doivent être spécifiés, implémentés et testés.
Pouvoir administratif	Aucune clé unique de mise à niveau, registre ou urgence ne peut modifier seule la condition composite ou le bénéficiaire.
Gel de l'EURC	Les pouvoirs de conformité de l'émetteur restent applicables ; le contrat ne peut neutraliser un gel du token.

12 Allocation contractuelle et réglementaire

Le nœud conclut la relation avec le participant et assume l'onboarding, l'offboarding, les contrôles d'identité, la passerelle SEPA et la conversion EUR et EURC. Il doit disposer des autorisations nécessaires ou recourir à un partenaire régulé habilité. Le périmètre exact dépend de sa juridiction et des contrats conclus.

Fonction	Responsable
Admission KYB et AML	Gestionnaire de nœud
Compte bancaire et SEPA	Nœud ou partenaire régulé du nœud
Conversion EUR et EURC	Nœud ou partenaire régulé du nœud
Conservation des graines A B C	Participant exclusivement
Séquestre du collatéral	Contrat Ethereum
État canonique et netting	Osnias Clearing sur Sei
Authentification entre chaînes	Vérificateur selon une gouvernance définie
Règlement du résultat	Nœuds selon les règles de clearing
Offboarding et remboursement	Gestionnaire de nœud

13 Invariants d'acceptation

- aucune graine ou clé privée du participant ne quitte son domaine de contrôle ;
- le nœud et Osnias ne peuvent pas initier seuls une opération depuis A, B ou C ;
- A, B et C proviennent de racines indépendantes et remplissent des fonctions distinctes ;
- le séquestre n'accepte que l'EURC natif Ethereum configuré officiellement ;
- le séquestre Ethereum ne calcule jamais le netting ;
- le résultat appliqué sur Ethereum provient d'un état Sei authentifié et lié au cycle actif ;
- aucun retrait n'est possible pendant un gel, une contestation ou une obligation active ;
- toute libération aboutit à C et jamais à une destination fournie au dernier moment ;
- la réconciliation post-clearing rapproche positions Sei, agrégats du nœud et soldes Ethereum ;
- l'état RÉVOQUÉ interdit définitivement toute nouvelle exposition tout en préservant l'historique.

14 Articulation avec le Livre 5 Sécurité

Le Livre 5 demeure la référence normative pour les contrôles qui protègent ce parcours. Il couvre notamment l'insuffisance d'une seule clé, l'indépendance des domaines A B C, la condition composite de libération, l'intégrité des registres, la protection contre le rejeu, le renouvellement et la révocation. Le présent Livre 6 applique ces exigences au parcours client sans dupliquer leur analyse de sécurité. Les preuves d'implémentation, les tests adversariaux et la revue indépendante demeurent nécessaires avant toute mise en production.

15 Conclusion

Le Livre 6 complète le corpus Osnias Clearing par sa couche d'exécution opérationnelle. Le gestionnaire de nœud porte la relation client, l'admission et la passerelle EUR EURC ; le participant conserve exclusivement ses domaines A B C ; Ethereum séquestre l'EURC natif ; Sei porte l'état canonique du clearing et le netting. Cette répartition maintient la séparation des responsabilités, la conservation autonome des clés et la vérifiabilité du collatéral, tout en organisant un parcours d'entrée et de sortie cohérent avec les Livres précédents.