OSNIAS CLEARING

https://www.osnias-clearing.com/osniasid/

contact@osnias-clearing.com

Osnias-ID :

Un Identifiant de compte de compensation et référence interchaînes

Livre I · Version 3.0 · Version de travail du 26 septembre 2026

Titre	**Un Identifiant de compte de compensation et référence interchaînes**
Auteur	**Denis Bouzon**
ORCID	**0009-0007-8894-8902**
Site web	**https://www.osnias-clearing.com/osniasid/**
Contact	**contact@osnias-clearing.com**
Version	**Version 3.0 · Version de travail · 26 septembre 2026**
Licence	**Creative Commons Attribution 4.0 International (CC BY 4.0)**
DOI ZENODO	**https://zenodo.org/uploads/22978105**

Abstract

Osnias-ID (OID) is a project-specific internal identifier for clearing accounts within the Osnias Clearing network. Release 2.0 extends the identifier from 16 to 19 decimal digits and makes two clearing properties intrinsic to the identifier: the ISO 4217 numeric currency code and the clearing-cycle duration expressed in weeks. The canonical format is KK-NNN-MMM-WW-SSSSSSS-XX. This enables a clearing account to be structurally bound to both its monetary rail and its clearing-room cycle before admission to escrow, payment messaging or settlement workflows.

The complete 19-digit value fits within an unsigned 64-bit integer. Implementations may therefore store the canonical numeric OID in a uint64 / 8-byte machine word while presenting the same value to users in the hyphenated decimal form. Currency, cycle, checksum and registry status remain independent admission controls: a correct checksum alone never proves eligibility.

Osnias-ID is not a legal-entity identifier, bank account number, wallet address, regulatory authorization number, security or token. The authoritative legal/KYC mapping remains in the controlled registry layer.

Keywords

Osnias Clearing, Osnias-ID, Clearing Account Identifier, Multi-Chain Clearing, ISO 4217, Clearing Cycle, Escrow, Currency Binding, uint64, 8-byte Identifier, MOD-97 Checksum, Participant Registry, Wallet Identity, KYC, KYB, AML, ISO 20022, Institutional Blockchain

contact@osnias-clearing.com

Résumé

Osnias-ID (OID) est un identifiant interne propre au projet, destiné aux comptes de compensation du réseau Osnias Clearing. L'évolution du format a porté sa longueur de 16 à 19 chiffres décimaux et intégré deux caractéristiques de la compensation à l'identifiant lui-même : le code numérique de devise ISO 4217 et la durée du cycle de compensation, exprimée en semaines. Le format canonique est KK-NNN-MMM-WW-SSSSSSS-XX. Un compte de compensation est ainsi structurellement rattaché à sa filière de compensation en devise et à son cycle de chambre de compensation avant toute admission aux processus d'escrow (séquestre), de messagerie de paiement ou de règlement.

La valeur complète à 19 chiffres tient dans un entier non signé de 64 bits. Les implémentations peuvent donc stocker la valeur numérique canonique de l'OID dans un uint64, soit un mot machine de 8 octets, tout en présentant cette même valeur aux utilisateurs sous forme décimale avec tirets. La devise, le cycle, la clé de contrôle et le statut au registre constituent des contrôles d'admission indépendants : une clé de contrôle correcte ne prouve jamais, à elle seule, l'éligibilité.

Osnias-ID n'est ni un identifiant d'entité juridique, ni un numéro de compte bancaire, ni une adresse de portefeuille, ni un numéro d'agrément réglementaire, ni un titre financier, ni un jeton. La correspondance de référence avec l'identité juridique et les données de connaissance du client (KYC) demeure dans la couche de registre à accès contrôlé.

Mots-clés

Osnias Clearing, Osnias-ID, identifiant de compte de compensation, compensation multichaînes, ISO 4217, cycle de compensation, escrow, rattachement à la devise, uint64, identifiant sur 8 octets, clé de contrôle MOD-97, registre des participants, identité associée au portefeuille, KYC, KYB, lutte contre le blanchiment (AML), ISO 20022, blockchain institutionnelle

Table des matières

1. Intention de conception initiale et raison d'être d'Osnias-ID

Osnias-ID a été conçu pour fournir à Osnias Clearing une référence compacte, indépendante des chaînes et utilisable de manière cohérente dans un environnement de compensation multichaînes. La version 3.0 préserve cet objectif tout en intégrant directement à l'identifiant deux attributs essentiels à la sécurité de la compensation : la devise et le cycle.

1.1 Référence de compensation indépendante des chaînes

L'identifiant ne dépend ni du système d'adressage, ni du modèle de compte, ni des conventions techniques d'une blockchain particulière. L'adresse technique du portefeuille ou de l'escrow peut changer selon des procédures contrôlées, sans modification de l'identité juridique associée au compte.

1.2 Messagerie compacte et routage déterministe

Au lieu de transporter des dossiers d'identité complets ou de répéter des métadonnées propres à chaque chaîne, le protocole peut transmettre l'OID et obtenir les informations détaillées sur le participant par résolution dans le registre. La version 3.0 permet en outre au composant destinataire de déduire directement de l'OID la filière en devise et le cycle de compensation visés, avant toute consultation du registre ou exécution.

1.3 Prévention des erreurs de routage monétaires et temporelles

Un compte de compensation valide pour une devise ou un cycle de chambre de compensation ne doit pas être admis implicitement dans un autre. La version 3.0 traite donc la devise et le cycle comme des invariants du protocole, plutôt que comme des métadonnées facultatives de base de données.

OBJECTIF DE CONCEPTION
Un compte de compensation est identifié non seulement par son attribution dans le registre, mais aussi par la filière en devise et le cycle de compensation pour lesquels son dispositif d'escrow a été créé.

2. Objet et périmètre

- **Identification des participants et des comptes de compensation, et consultation du registre.**
- **Association entre un OID et la ou les adresses techniques autorisées.**
- **Rattachement de l'OID à un code numérique de devise ISO 4217.**
- **Rattachement de l'OID à une durée de cycle de compensation autorisée, exprimée en semaines.**
- **Contrôle d'admission des demandes relatives à l'escrow, au paiement, à la compensation et au règlement.**
- **Piste d'audit de la création de l'identifiant, des associations de portefeuilles, des changements de cycle de vie et des contrôles de routage.**

3. Statut de la spécification

Ce document constitue le Livre I du corpus de référence technique et fonctionnel d'Osnias Clearing. Cette version de travail 3.0, datée du 26 septembre 2026, révise la spécification publiée le 11 septembre 2026 [12]. Le format à 19 chiffres et la règle de génération de la clé de contrôle restent inchangés. La spécification antérieure avait introduit la transition depuis le format initial à 16 chiffres. Cette version précise la validation, la représentation et la sémantique du registre ; elle ne revendique aucune certification externe, aucun agrément réglementaire ni aucun nouveau dépôt dans une archive.

4. Structure de l'identifiant — Version 3.0

KK-NNN-MMM-WW-SSSSSSS-XX

Champ	Longueur	Autorité	Signification
KK	2	Osnias Clearing	Code de blockchain / réseau prenant en charge l'escrow.
NNN	3	Osnias Clearing	Code de serveur / nœud d'escrow autorisé.
MMM	3	ISO 4217 / validation Osnias	Code numérique de devise ISO 4217 utilisé par le compte de compensation.
WW	2	Osnias Clearing	Cycle de compensation en semaines entières ; par exemple 01, 04, 13.
SSSSSSS	7	Serveur de registre	Valeur de compte séquentielle ou unique sous contrôle, attribuée par le serveur dans l'espace de noms KK/NNN/MMM/WW.
XX	2	Serveur de registre	Clé de contrôle MOD-97 calculée sur les 17 chiffres de données précédents.

La représentation canonique comprend 19 chiffres décimaux, hors séparateurs. Les zéros initiaux sont significatifs dans la forme destinée à la lecture humaine. Les 17 chiffres de données sont constitués par KK || NNN || MMM || WW || SSSSSSS. XX complète l'identifiant.

5. Rattachement à la devise et au cycle de compensation

MMM et WW ne sont pas de simples libellés descriptifs. Ce sont des champs de routage essentiels à la sécurité. Ils sont définis lors de la création du compte de compensation et du dispositif d'escrow qui lui est associé.

5.1 Champ de devise MMM

MMM contient le code numérique ISO 4217 à trois chiffres de la devise utilisée par la filière de compensation. Exemples : 840 pour USD, 978 pour EUR, 756 pour CHF et 156 pour CNY. Osnias Clearing tient à jour la liste des devises acceptées. Un OID ne doit pas être admis dans une filière de compensation dont la devise configurée diffère de MMM. [1, 2]

MMM identifie la devise de dénomination du compte de compensation. Il n'identifie ni un jeton de collatéral, ni un émetteur, ni une adresse de contrat, ni un instrument de règlement. Le dispositif d'escrow doit enregistrer séparément la devise de dénomination applicable et l'identité ainsi que l'éligibilité de l'actif de collatéral ou de règlement. Toute règle de valorisation, de conversion ou d'acceptation du collatéral relève des dispositions applicables à la chambre de compensation et au nœud concernés ; l'OID seul n'établit pas l'équivalence entre actifs.

5.2 Champ de cycle de compensation WW

WW exprime le cycle de compensation en semaines entières. Exemples : 01 = 7 jours, 04 = 28 jours, 13 = 91 jours. Seuls les cycles explicitement activés par Osnias Clearing sont valides. Ce champ n'ouvre pas, à lui seul, une chambre de compensation ; il rattache le compte à la configuration de cycle autorisée.

WW identifie une durée de cycle, et non une occurrence datée particulière ni une chambre de compensation unique. L'admission doit également vérifier la chambre et l'occurrence du cycle visées au regard du registre faisant autorité et de la configuration de la chambre.

INVARIANT D'ADMISSION À LA COMPENSATION

Devise OID = devise de dénomination configurée du dispositif d'escrow associé = devise de la filière de compensation ; cycle OID = cycle escrow configuré = cycle de la chambre de compensation. Toute divergence doit entraîner un rejet par défaut avant l'émission (mint), l'admission d'un paiement ou le règlement. Cet invariant n'assimile pas le code de devise à un jeton de collatéral ou à un actif de règlement particulier.

Une même entité juridique peut donc détenir plusieurs OID dans une même devise si elle participe à différents cycles de compensation, ou plusieurs OID pour différentes devises au sein d'un même cycle.

6. Séparation des couches d'identité et d'adressage

Un OID identifie un compte de compensation. Une adresse de portefeuille identifie une destination technique ou un compte signataire. Un enregistrement d'entité juridique identifie l'entreprise ou l'institution à laquelle sont rattachés un ou plusieurs comptes de compensation. Ces couches doivent rester distinctes.

- **Identité juridique : entreprise ou institution et ses identifiants externes reconnus.**
- **Osnias-ID : identifiant de compte de compensation intégrant la devise et le cycle de compensation.**
- **Adresse de portefeuille / d'escrow : point d'exécution technique.**
- **Justificatifs KYC/KYB : données d'identité et de vérification à accès contrôlé.**

7. Architecture du registre

Le registre Osnias demeure la couche de résolution faisant autorité entre un OID et les données opérationnelles autorisées du participant. La version 3.0 ne transfère pas l'identité juridique ni les justificatifs KYC/KYB sur la blockchain au seul motif que l'OID peut y être encodé.

- **OID canonique et champs KK, NNN, MMM, WW et SSSSSSS décodés.**
- **Associations actuellement autorisées avec les adresses de portefeuilles et d'escrow.**
- **Statut du participant : actif, suspendu, révoqué, en attente ou archivé.**
- **Statut et horodatage de la vérification d'identité.**
- **Identifiants externes facultatifs tels que LEI, UID/CHE ou références nationales d'immatriculation des entreprises.**
- **Enregistrements d'audit relatifs à la création, aux mises à jour, à la révocation et à l'historique des associations.**

Le registre doit distinguer les éléments probants historiques immuables de l'état opérationnel courant utilisé pour l'admission. Une association historique ne prouve pas qu'une adresse reste autorisée ni qu'un compte de compensation possède actuellement le statut ACTIVE. Le modèle on-chain prévu est décrit à la section 22.1.

PÉRIMÈTRE DE CONFIDENTIALITÉ

Les justificatifs KYC/KYB personnels ou confidentiels ne devraient pas être inscrits sur une blockchain publique au seul motif que l'OID est utilisé on-chain ou dans un message de compensation.

8. Contrôle d'accès — Osnias-ID requis pour les participants à la compensation

1. Analyser l'OID à 19 chiffres et valider sa structure.
2. Valider la clé de contrôle MOD-97.
3. Décoder MMM et le comparer à la devise de dénomination configurée du dispositif d'escrow et de la filière de compensation visés.
4. Décoder WW et le comparer au cycle de la chambre de compensation visée.
5. Résoudre l'OID dans le registre faisant autorité et vérifier le statut ACTIVE.
6. Vérifier l'association avec le portefeuille / l'escrow ainsi que toute règle d'éligibilité liée au prêteur, au réseau, à la juridiction ou à la transaction.
7. Admettre l'opération uniquement après ces contrôles.

PRINCIPE DE REJET PAR DÉFAUT
Un OID de structure valide doté d'une clé de contrôle correcte ne suffit pas. La devise, le cycle, l'état du registre et les associations d'adresses opérationnelles doivent tous être valides.

9. Une entité juridique et plusieurs comptes de compensation Osnias-ID

Un OID n'est pas un identifiant d'entreprise. Il identifie un compte de compensation rattaché à un participant identifié. Une entreprise peut donc détenir plusieurs OID, tous reliés dans le registre à la même entité juridique.

Entité juridique	Devise	Cycle	Exemple d'utilisation
Entreprise A	USD (840)	13 semaines	Compte de compensation ORUSD à 91 jours
Entreprise A	USD (840)	04 semaines	Compte de compensation USD à 28 jours
Entreprise A	EUR (978)	13 semaines	Compte de compensation OEURO à 91 jours

10. Utilisation inter-chaînes

L'OID demeure une référence interne de compensation interchaînes. KK identifie l'affectation à un réseau ou à une filière. L'identifiant ne confère pas, à lui seul, de droits d'exécution interchaînes ; chaque opération propre à une chaîne reste soumise aux contrats concernés, aux permissions des contrôleurs, à l'état de l'escrow et à celui du registre.

11. Interopérabilité avec les identifiants externes

Les identifiants externes identifient ou décrivent l'entité juridique concernée ; ils ne remplacent pas l'identifiant de compte de compensation Osnias. Les références LEI relèvent du cadre GLEIF [6] ; les références suisses UID/CHE concernent l'identification des entreprises [10]. Toute métadonnée de statut réglementaire doit mentionner sa source et sa date de vérification. Les informations du registre FINMA constituent une référence à un instant donné et n'impliquent aucune approbation d'Osnias [7].

Référence externe	Utilisation possible	Limite
LEI	Rapprochement avec l'entité juridique	Osnias n'émet pas de LEI.
UID / CHE suisse	Rapprochement avec une entreprise suisse	Osnias n'attribue pas de numéros UID.
Données du registre FINMA	Métadonnées de statut réglementaire lorsqu'elles sont publiques et pertinentes	Aucune approbation ni autorisation de la FINMA n'est implicite.

Référence externe	Utilisation possible	Limite
Autres identifiants nationaux	Rapprochement propre à chaque juridiction	Sous réserve des contraintes de source et de confidentialité.

12. Articulation avec ISO 20022 et ISO 4217

Osnias-ID n'est pas un identifiant ISO 20022 et n'est pas présenté comme un élément de données certifié ISO 20022. Les concepts ISO 20022 peuvent servir de références d'interopérabilité pour établir les correspondances entre données de participant, de compte, d'agent ou de message de paiement. [3, 4]

La version 3.0 utilise le code numérique de devise ISO 4217 à trois chiffres comme base sémantique de MMM. Cet usage ne fait pas d'Osnias-ID une norme ISO et n'implique aucune approbation par l'ISO. Osnias Clearing demeure responsable du choix des codes de devise activés pour les filières de compensation. [1, 2]

13. Hiérarchie d'attribution

Niveau	Champ	Autorité	Objectif du contrôle
1	KK	Osnias Clearing	Attribuer et tenir à jour les codes de réseau / filière.
2	NNN	Osnias Clearing	Attribuer les codes de serveur / nœud d'escrow autorisés.
3	MMM	Référence ISO 4217 + politique Osnias	Rattacher le compte à une filière en devise activée. Choix de l'utilisateur final parmi les devises activées par Osnias ; validation lors de l'émission.
4	WW	Osnias Clearing	Rattacher le compte à un cycle de compensation activé. Choix de l'utilisateur final parmi les cycles activés par Osnias ; validation lors de l'émission.
5	SSSSSSS	Serveur de registre	Émettre des valeurs de compte uniques dans l'espace de noms KK/NNN/MMM/WW.
6	XX	Serveur de registre	Calculer les chiffres de contrôle d'intégrité de manière déterministe.

INVARIANT D'AUTORITÉ

KK et NNN sont attribués par Osnias. MMM doit être un code numérique de devise ISO 4217 activé. WW doit correspondre à un cycle de compensation activé. SSSSSSS est attribué par le serveur de registre. XX est calculé par ce serveur. Aucun champ ne peut être réaffecté implicitement par un portefeuille, une interface utilisateur ou un contrat intelligent en aval.

14. Représentation machine — 19 chiffres décimaux dans un uint64

L'OID canonique complet comprend 19 chiffres décimaux. La valeur maximale possible sur 19 chiffres est 9 999 999 999 999 999 999, inférieure au maximum d'un uint64, soit 18 446 744 073 709 551 615. Tout OID canonique au format de la version 3.0 tient donc dans un entier non signé de 64 bits.

Représentation	Taille	Finalité
Affichage canonique lisible	19 chiffres décimaux + séparateurs	Échange lisible et documentation.

Représentation	Taille	Finalité
Valeur numérique canonique	19 chiffres décimaux, sans séparateurs	Analyse déterministe et validation de la clé de contrôle.
Stockage machine	uint64	Capacité de représentation sur 64 bits (8 octets) ; la taille effective de stockage et de transport dépend de l'implémentation et de l'encodage.
Représentation hexadécimale	Jusqu'à 16 chiffres hexadécimaux	Représentation de la même valeur uint64 à des fins de diagnostic.

Les zéros initiaux font partie de la représentation canonique, mais ne sont pas conservés par le formatage ordinaire des entiers. Tout composant convertissant un uint64 vers la forme lisible doit compléter la valeur à gauche par des zéros jusqu'à obtenir exactement 19 chiffres décimaux, avant d'insérer les séparateurs.

La borne du uint64 définit la plage des valeurs représentables, et non une taille universelle de stockage blockchain ou de message. Dans l'ABI standard de Solidity, un argument uint64 est complété à gauche par des octets nuls jusqu'à 32 octets. L'encodage compact (packed encoding) et l'organisation du stockage du contrat constituent des choix d'implémentation distincts [9].

PRINCIPE D'ENCODAGE

Les formes décimale et hexadécimale représentent le même entier de 64 bits. La sémantique de sécurité repose sur l'agencement des champs et les règles de validation, et non sur le choix de la base d'affichage.

15. API et modèle de résolution

Exemple de requête de consultation :

```
GET /api/osnias-id/01-001-840-13-0000001-18
```

Exemple de réponse :

```
{
  "osnias_id": "01-001-840-13-0000001-18",
  "status": "ACTIVE",
  "checksum_valid": true,
  "currency_numeric": "840",
  "cycle_weeks": 13,
  "wallets": [],
  "external_identifiers": {}
}
```

Les requêtes et réponses d'API doivent transporter l'OID sous forme de chaîne JSON, en préservant ses chiffres décimaux et ses zéros initiaux. L'exemple ci-dessus illustre une structure de réponse ; il ne prouve ni le déploiement d'un point d'accès opérationnel ni qu'une liste de portefeuilles vide autorise l'admission. Ne pas convertir l'OID par l'intermédiaire d'un nombre à virgule flottante ; utiliser une arithmétique entière exacte ou une arithmétique modulaire chiffre par chiffre. L'interopérabilité JSON avec les implémentations binary64 courantes est limitée aux entiers exacts compris entre −(2^53−1) et 2^53−1 [8].

16. Spécification normative de la clé de contrôle

La version 3.0 conserve la règle d'intégrité MOD-97 à deux chiffres, étendue aux 17 chiffres de données du nouveau format.

16.1 Données d'entrée

Accepter uniquement la forme canonique avec tirets ou une chaîne composée d'exactement 19 chiffres décimaux ASCII, conformément à la section 18. Supprimer les cinq séparateurs seulement après avoir vérifié leur position. Soit B la chaîne décimale à 17 chiffres : B = KK || NNN || MMM || WW || SSSSSSS.

16.2 Calcul

Ajouter deux chiffres zéro à B pour obtenir B00.

Interpréter B00 comme un entier décimal positif ou nul.

Calculer r = B00 mod 97.

Calculer XX = 98 - r.

Encoder XX sur exactement deux chiffres décimaux, avec un zéro initial si nécessaire.

16.3 Validation

Soit I l'identifiant complet à 19 chiffres B || XX. La validation doit recalculer la valeur attendue de XX selon la section 16.2 et la comparer exactement à la valeur reçue sur deux chiffres. La valeur générée de XX est comprise entre 02 et 98. La condition supplémentaire I mod 97 = 1 est un contrôle de cohérence ; elle ne doit pas remplacer la comparaison exacte, car une valeur non canonique sur deux chiffres peut satisfaire la même condition de reste.

Par exemple, 01-001-840-13-0000007-97 possède la clé de contrôle canonique. Remplacer 97 par 00 donne encore I mod 97 = 1, mais doit entraîner un rejet, car 00 diffère de la clé recalculée. Cette précision aligne la section 16.3 sur la comparaison exacte déjà requise par le pseudocode de référence.

PRÉCISION RELATIVE À LA NORMALISATION
Il s'agit de la règle normative de clé de contrôle Osnias-ID pour la version 3.0. Elle utilise l'arithmétique MOD-97 et peut être reproduite indépendamment. ISO/IEC 7064:2003 constitue une référence informative [5] ; sa citation ne vaut pas revendication de conformité formelle. La clé de contrôle n'est ni une signature cryptographique, ni un code d'authentification de message (MAC), ni une preuve d'inscription au registre.

17. Vecteurs de test de la clé de contrôle

KK	NNN	MMM	WW	SSSSSSS	XX	Représentation canonique
01	001	840	13	0000001	18	01-001-840-13-0000001-18
01	001	978	04	0000002	19	01-001-978-04-0000002-19
02	023	756	01	1234567	83	02-023-756-01-1234567-83
12	034	156	13	7654321	54	12-034-156-13-7654321-54
99	099	840	52	9999999	28	99-099-840-52-9999999-28

17.1 Exemple détaillé

Pour l'OID 01-001-840-13-0000001-18 :

```
B      = 01001840130000001
B00    = 0100184013000000100
r      = B00 mod 97 = 80
XX     = 98 - 80 = 18
I      = 0100184013000000118
I mod 97 = 1   -> VALID
```

17.2 Détection d'erreurs

La clé de contrôle vise à détecter les erreurs courantes de transcription et de saisie, y compris les modifications accidentelles des chiffres de devise ou de cycle intégrés. Elle ne remplace pas la validation du registre, de l'escrow, de la devise ou du cycle.

Les vecteurs de la section 17 et de l'annexe C établissent uniquement la validité du format et de la clé de contrôle. Leur utilisation ne signifie pas que les valeurs KK, NNN, de devise ou de cycle illustrées sont activées en production, ni que le compte existe dans un registre.

18. Règles de formatage

- **Représentation canonique : KK-NNN-MMM-WW-SSSSSSS-XX.**
- **Valeur numérique canonique : 19 chiffres décimaux sans séparateurs.**
- **Les zéros initiaux sont significatifs dans la représentation canonique.**
- **Les espaces sont interdits dans la valeur canonique.**
- **La clé de contrôle est calculée uniquement à partir des 17 premiers chiffres de données.**
- **Les séparateurs de présentation sont exclus du calcul de la clé de contrôle.**
- **Lors de la conversion d'un uint64 vers la forme affichée, compléter à gauche jusqu'à 19 chiffres avant de séparer les champs.**

La syntaxe d'entrée acceptée est [0-9]{19} ou [0-9]{2}-[0-9]{3}-[0-9]{3}-[0-9]{2}-[0-9]{7}-[0-9]{2}, avec correspondance sur la totalité de l'entrée. Rejeter les séparateurs mal placés, les espaces, les signes et les chiffres non ASCII. Les règles d'attribution, les codes activés, l'état courant du registre et le contexte cible doivent ensuite être vérifiés indépendamment.

19. Unicité et réémission

Le champ SSSSSSS à sept chiffres offre 10 000 000 de valeurs locales pour chaque espace de noms KK × NNN × MMM × WW. Lorsqu'un serveur approche de l'épuisement des valeurs disponibles pour une devise et un cycle donnés, Osnias peut attribuer un autre code de serveur / nœud NNN, plutôt que de réutiliser des identifiants déjà émis.

La capacité de 10 000 000 inclut 0000000. Toute valeur réservée par la politique d'attribution réduit la capacité utilisable et doit être documentée. Les valeurs historiques restent réservées ; l'attribution d'un nouveau code de nœud ne transfère pas les responsabilités juridiques ou opérationnelles d'un nœud existant.

PRINCIPE DE NON-RÉUTILISATION
Un OID déjà émis devrait rester historiquement unique, même après clôture, révocation ou migration. Les valeurs révoquées devraient rester réservées ou être conservées sous forme d'enregistrements de retrait définitif (tombstones).

20. États du cycle de vie

État	Signification	Admission à la compensation
PENDING	Enregistrement créé, mais pas entièrement activé.	Rejetée
ACTIVE	Compte, rattachement devise/cycle et association de portefeuille valides.	Éligible, sous réserve des autres règles
SUSPENDED	Temporairement désactivé.	Rejetée
REVOKED	Retiré définitivement.	Rejetée
ARCHIVED	Enregistrement historique conservé pour l'audit.	Rejetée

21. Modèle de sécurité

- **Rejeter l'opération par défaut (fail closed) lorsque la résolution dans le registre est indisponible ou ambiguë.**
- **Valider la structure à 19 chiffres et la clé de contrôle avant les étapes de résolution coûteuses.**
- **Comparer MMM à la devise de dénomination configurée du dispositif d'escrow et de la chambre de compensation avant l'admission.**
- **Comparer WW au cycle de l'escrow et de la chambre de compensation avant l'admission.**
- **Exiger le statut ACTIVE dans le registre, indépendamment de la validité de la clé de contrôle.**
- **Vérifier les associations courantes avec les portefeuilles / escrows.**
- **Empêcher la génération côté client de valeurs OID faisant autorité.**
- **Journaliser la création, les associations, les remplacements, les suspensions, les révocations et les changements de configuration.**
- **Protéger les données KYC/KYB confidentielles indépendamment de la résolution publique des OID.**

DÉFENSE EN PROFONDEUR
Le rattachement à la devise, le rattachement au cycle, la validation de la clé de contrôle, l'inscription au registre et l'autorisation d'escrow / d'adresse sont des contrôles distincts. La compromission d'une couche ne doit pas autoriser implicitement une opération de compensation incompatible.

22. Périmètre des contrats intelligents

Lorsqu'un OID est référencé par un contrat intelligent (smart contract), la version 3.0 permet une représentation compacte en uint64. Le contrat peut décoder les champs sémantiques nécessaires au routage déterministe et aux contrôles d'admission, notamment MMM et WW. Les contrats intelligents ne devraient pas devenir le référentiel faisant autorité pour les informations juridiques ou KYC/KYB confidentielles. Une valeur uint64 n'implique pas un encodage ABI standard sur huit octets ; voir la section 14 [9].

Un contrat recevant un OID pour une opération de compensation devrait rejeter l'opération si la devise ou le cycle décodés diffèrent de la filière configurée, même si une application en amont ou une base SQL indique une correspondance différente.

22.1 Architecture de contrôle prévue à deux registres on-chain

L'architecture de contrôle Osnias-ID prévue comprend deux composants de registre on-chain complémentaires. Sur le réseau d'escrow, un oracle de registre vérifierait et enregistrerait chaque compte d'escrow nouvellement admis et l'associerait à son Osnias-ID. Sur Sei, un second registre enregistrerait l'association correspondante entre l'Osnias-ID et l'adresse locale de compensation 0x. Cette section décrit une orientation de conception ; elle ne prouve ni un déploiement ni la réalisation d'un audit.

Les registres prévus conservent un historique alimenté uniquement par ajout (append-only). Un événement enregistré ne doit pas être écrasé ni réaffecté par une opération ultérieure du registre. Les changements d'adresse autorisée, les suspensions, les révocations et les autres changements du cycle de vie sont représentés par de nouveaux événements autorisés qui préservent les éléments probants antérieurs. La résolution doit restituer l'association et le statut actuellement en vigueur, selon des règles explicites d'ordonnancement et d'autorisation ; une ancienne association ne doit pas rester éligible au seul motif qu'elle figure encore dans l'historique. Cette règle applicative dépend des hypothèses de finalité des réseaux sous-jacents ; elle ne constitue pas une affirmation inconditionnelle selon laquelle une blockchain ne pourrait jamais subir de réorganisation.

La conception à deux registres complète les contrôles de clé, de devise, de cycle et de statut au registre. Avant toute utilisation opérationnelle, une spécification dédiée doit définir la source faisant autorité pour chaque état, l'ordonnancement des événements, le rapprochement entre registres, les exigences de finalité et le traitement des divergences. La résolution doit entraîner un rejet par défaut lorsque l'état en vigueur est indisponible ou ambigu. L'architecture détaillée des oracles, les interfaces, le processus d'enregistrement, l'implémentation et le code source restent l'objet d'une publication technique ultérieure.

23. Intégration dans les messages de paiement

Les messages de paiement peuvent transporter les Osnias-ID de l'émetteur et du destinataire comme références de comptes de compensation. Les implémentations doivent préserver les chaînes exactes des identifiants et valider la devise, le cycle, le statut courant au registre et les associations d'adresses autorisées avant l'admission. Un message doit également identifier sa chambre de compensation cible et l'occurrence datée du cycle ; ces éléments ne sont pas entièrement encodés par MMM et WW seuls.

Lorsqu'une interopérabilité ISO 20022 est visée, l'implémentation doit documenter les définitions de messages, les versions et les correspondances de champs retenues [3, 4]. Cette spécification n'enregistre pas de nouvel élément de données ISO 20022 et n'établit pas la conformité des messages. La présence d'un Osnias-ID dans un message de paiement n'exécute pas le règlement et ne prouve pas son caractère juridiquement définitif.

24. Interopérabilité institutionnelle

Pour les banques, prestataires d'escrow, prêteurs ou partenaires réglementés, l'OID peut servir de clé interne au réseau de compensation pour rapprocher les adresses techniques des contreparties reconnues par les institutions. Le rattachement à la devise et au cycle permet à un partenaire de déterminer qu'un compte a été créé pour le même contexte monétaire et temporel de compensation que l'opération demandée.

25. Confidentialité et protection des données

- **Appliquer la minimisation des données et ne conserver que les champs nécessaires à la finalité de compensation.**
- **Séparer les données publiques d'identification des justificatifs d'identité confidentiels.**
- **Éviter d'inscrire directement sur la blockchain des adresses personnelles, adresses électroniques, numéros de téléphone ou pièces d'identité.**
- **Appliquer des contrôles d'accès et une limitation des finalités aux consultations du registre portant sur des données non publiques.**
- **Conserver les éléments probants d'audit nécessaires sur le plan juridique ou opérationnel, sans exposer de données personnelles superflues.**

Conserver les justificatifs d'identité hors chaîne ne rend pas, à lui seul, un OID ou une association de portefeuille anonyme. Un identifiant peut rester une donnée personnelle lorsqu'il peut être relié à une personne physique identifiable. Il convient d'évaluer les possibilités de rapprochement, les droits d'accès, la conservation et les obligations applicables en matière de protection des données, tant pour les données publiques que pour celles du registre à accès contrôlé. Les orientations de la CNIL relatives à la blockchain et aux données personnelles constituent une référence informative [11].

26. Auditabilité et gouvernance

- **Audit structurel : format à 19 chiffres, longueur des champs, bornes du uint64 et clé de contrôle.**
- **Audit du routage : décodage de MMM/WW et comparaison avec la devise de dénomination de l'escrow, la chambre de compensation et la configuration du cycle daté.**
- **Audit du registre : autorité d'attribution, unicité, cycle de vie et historique des associations de portefeuilles.**
- **Audit de sécurité : administration privilégiée, autorisations de l'API, comportement de rejet par défaut et journalisation.**
- **Audit du protocole : application du principe « sans OID valide, aucune demande de compensation » et des invariants de devise et de cycle.**

Annexe A — Pseudocode de validation machine

```
function validateOsniasId(input, expectedCurrency, expectedCycle):
    if not canonicalSyntax(input): return false
    digits = removeCanonicalHyphens(input)
    payload = digits[0:17]
    receivedXX = digits[17:19]
    kk  = digits[0:2]
    nnn = digits[2:5]
    mmm = digits[5:8]
    ww  = digits[8:10]
    sequence = digits[10:17]

    remainder = mod97Digits(payload + "00")
    expectedXX = leftPad2(98 - remainder)
```

```
if receivedXX != expectedXX: return false
if mod97Digits(digits) != 1: return false
if kk == "00": return false
if mmm != expectedCurrency: return false
if exactInteger(ww) != expectedCycle: return false

oid64 = uint64(exactInteger(digits))
record = registry.resolveCurrentOrFail(oid64)
if record is missing or unavailable or ambiguous: return false
if record.status != ACTIVE: return false
if not record.authorizesCurrentAddress(): return false
return true
```

canonicalSyntax applique les motifs ASCII de la section 18 à la totalité de l'entrée. mod97Digits traite les chiffres décimaux selon r = (10 × r + digit) mod 97, en partant de zéro ; aucune conversion en virgule flottante n'est utilisée. expectedCurrency est une chaîne de trois chiffres et expectedCycle est un entier. L'admission en production doit également vérifier les valeurs KK/NNN/MMM/WW activées, l'escrow et l'actif visés, la chambre de compensation, l'occurrence datée du cycle, le réseau, le prêteur et toute autre condition d'éligibilité applicable. Tout contrôle échoué, indisponible ou ambigu doit entraîner le rejet de l'opération.

Annexe B — Règles d'attribution des codes de chaîne / réseau KK

- **KK contient exactement deux chiffres décimaux. KK=00 reste définitivement réservé à la valeur nulle / non attribuée.**
- **KK est attribué et contrôlé par Osnias Clearing comme code d'identification d'un domaine de blockchain / réseau pris en charge.**
- **Les métadonnées détaillées du réseau sont conservées séparément afin de pouvoir évoluer sans modifier la largeur du champ OID.**
- **Les valeurs KK obsolètes ou retirées restent documentées dans l'historique et ne doivent pas être réattribuées implicitement.**

Annexe C — Vecteurs de test de référence

01-001-840-13-0000001-18 FORMAT ET CLÉ DE CONTRÔLE VALIDES

01-001-978-04-0000002-19 FORMAT ET CLÉ DE CONTRÔLE VALIDES

02-023-756-01-1234567-83 FORMAT ET CLÉ DE CONTRÔLE VALIDES

12-034-156-13-7654321-54 FORMAT ET CLÉ DE CONTRÔLE VALIDES

99-099-840-52-9999999-28 FORMAT ET CLÉ DE CONTRÔLE VALIDES

01-001-840-13-0000007-97 FORMAT ET CLÉ DE CONTRÔLE VALIDES

01-001-840-13-0000007-00 INVALIDE : clé de contrôle non canonique, malgré un reste égal à 1

Un OID dont la clé de contrôle est valide doit néanmoins être rejeté lorsque le registre est indisponible, absent ou ambigu, lorsque le statut est suspendu ou révoqué, ou lorsque la devise, le cycle, la chambre ou l'autorisation d'adresse ne correspondent pas à l'opération visée.

Les implémentations devraient intégrer ces vecteurs aux tests automatisés. La modification d'un seul chiffre, y compris d'un chiffre de devise ou de cycle, devrait normalement invalider la clé de contrôle.

Annexe D — Normes et références externes

[1] ISO. ISO 4217 — Codes des devises. Référence du champ numérique de devise.

https://www.iso.org/iso-4217-currency-codes.html

[2] SIX. Global Financial Data Standards — Agence de maintenance ISO 4217 et listes courantes des devises et des fonds.

https://www.six-group.com/en/products-services/financial-information/market-reference-data/data-standards.html

[3] ISO. ISO 20022-1:2026 — Services financiers — Schéma universel de messages pour l'industrie financière — Partie 1 : Métamodèle.

https://www.iso.org/standard/20022-1

[4] ISO. ISO 20022-3:2026 — Services financiers — Schéma universel de messages pour l'industrie financière — Partie 3 : Modélisation.

https://www.iso.org/standard/20022-3

[5] ISO/IEC. ISO/IEC 7064:2003 — Technologies de l'information — Techniques de sécurité — Systèmes de caractères de contrôle. Référence informative.

https://www.iso.org/standard/31531.html

[6] GLEIF. The Legal Entity Identifier — Identification des entités juridiques fondée sur ISO 17442.

https://www.gleif.org/en/organizational-identity/lei-vlei/the-legal-entity-identifier-lei

[7] FINMA. Établissements, personnes et produits autorisés. Référence relative au statut réglementaire.

https://www.finma.ch/en/finma-public/authorised-institutions-individuals-and-products/

[8] Bray, T., dir. RFC 8259 — The JavaScript Object Notation (JSON) Data Interchange Format. Décembre 2017, section 6.

https://www.rfc-editor.org/rfc/rfc8259.html#section-6

[9] Documentation Solidity. Contract ABI Specification — Formal Specification of the Encoding.

https://docs.soliditylang.org/en/latest/abi-spec.html

[10] Administration fédérale des contributions. Unternehmens-Identifikationsnummer (UID) — Numéro d'identification des entreprises.

https://www.estv.admin.ch/de/unternehmens-identifikationsnummer-uid

[11] CNIL. Blockchain et RGPD : quelles solutions pour un usage responsable en présence de données personnelles ?

https://www.cnil.fr/fr/technologies/blockchain-et-rgpd-quelles-solutions-pour-un-usage-responsable-en-presence-de-donnees-personnelles

[12] Bouzon, Denis. Osnias-ID: A Clearing ID Account as Inter-chain Identifier. Publication du 11 septembre 2026. HAL hal-05746489, tel qu'indiqué sur la couverture du PDF publié.

PDF publié de référence — Osnias-ID

Références web consultées le 26 septembre 2026. Les vérifications opérationnelles de devise et de statut réglementaire doivent utiliser la source courante pertinente et enregistrer la date de vérification. Les références [3] à [5] désignent des normes ; elles ne constituent pas une évaluation de conformité d'Osnias.

Osnias-ID demeure un identifiant propriétaire du projet tant qu'un organisme externe de normalisation, un régulateur ou une autre autorité compétente n'en a pas explicitement décidé autrement. Les références à des normes externes sont des références d'interopérabilité et n'impliquent ni certification ni approbation.

Historique de l'évolution du format

- **Publication de la spécification de référence le 11 septembre 2026.**
- **Transition majeure du format de 16 à 19 chiffres décimaux.**
- **Remplacement de KK-NNN-AAAAAAAAA-XX par KK-NNN-MMM-WW-SSSSSSS-XX.**
- **Ajout de MMM comme champ de devise numérique ISO 4217 à trois chiffres.**
- **Ajout de WW comme champ de cycle de compensation à deux chiffres, exprimé en semaines entières.**
- **Remplacement de l'ancien champ de compte à neuf chiffres par une séquence à sept chiffres dans chaque espace de noms KK × NNN × MMM × WW, soit 10 000 000 de valeurs de séquence possibles avant les réservations prévues par la politique d'attribution.**
- **Définition de l'identifiant complet à 19 chiffres comme compatible avec un stockage machine en uint64 / 8 octets.**

- **Rattachement de la devise de l'OID à la devise de dénomination configurée du dispositif d'escrow et de la filière de compensation ; l'éligibilité du collatéral et de l'actif de règlement reste contrôlée séparément.**
- **Définition de l'invariant de cycle obligatoire : cycle OID = cycle escrow = cycle de la chambre de compensation.**
- **Extension des données de la clé de contrôle MOD-97 de 14 à 17 chiffres et publication de nouveaux vecteurs de test.**
- **Maintien de la validation du registre, du statut ACTIVE du cycle de vie et de l'autorisation d'adresse / d'escrow comme contrôles indépendants.**
- **Précision selon laquelle les champs de clé, de devise et de cycle ne remplacent pas les contrôles juridiques et KYC du registre.**
- **Maintien de la licence de publication CC BY 4.0 et des réserves explicites relatives à l'absence de certification et d'approbation.**

• Introduction de la conception prévue à deux registres on-chain pour les associations côté escrow et côté Sei. La révision de travail du 26 septembre précise la distinction entre les éléments probants historiques et l'autorisation actuellement en vigueur. L'architecture détaillée des oracles et des contrats intelligents ainsi que le code source restent réservés à une publication ultérieure.

Version 3.0 — Révision de travail du 26 septembre 2026

• Le format à 19 chiffres et la règle de génération de la clé de contrôle restent inchangés. Les cinq vecteurs de contrôle d'origine sont conservés.

• Précision de la comparaison exacte de la clé, de la syntaxe d'entrée, de l'arithmétique exacte et de la résolution avec rejet par défaut ; ajout d'un exemple de rejet de clé non canonique.

• Distinction entre devise de dénomination et identité de l'actif, ainsi qu'entre capacité du uint64 et encodages API et ABI.

• Précision du modèle de cycle de vie prévu pour le registre, rétablissement de la section 23 et harmonisation de la table des matières.

• Ajout de références traçables et correction d'incohérences éditoriales. La source publiée conserve sa date et sa référence HAL d'origine ; aucun nouvel identifiant DOI ou HAL n'est attribué par cette version de travail 3.0.

JUSTIFICATION DE L'ÉVOLUTION MAJEURE

Le format retenu dans la version 3.0 intègre la compatibilité monétaire et temporelle de la compensation dans l'OID canonique lui-même, au lieu de la laisser dans des métadonnées applicatives modifiables. Il préserve une représentation machine compacte et la séparation entre identité juridique, compte de compensation et adresse d'exécution technique.

FIN DU DOCUMENT