

Klérotèrion

Démocratie directe horizontale à l'échelle humaine — documentation complète du système

Version 1.1 — 19 septembre 2026 — alignée sur la spécification cellules v14

Klérotèrion — Floating Coconuts

Licence AGPL-3.0 — document de travail

Statut de ce document : présentation de référence, non normative. Le texte qui fait foi est la spécification *spec-cellules-v14.md* (Klérotèrion). En cas de divergence sur une valeur, un seuil ou une procédure, c'est la spécification qui compte, jamais ce document. Les valeurs sont répétées ici pour la lecture, ce qui est précisément la source des contradictions passées.

Sommaire

1. Le nom : Klérotèrion

- 1.1 La machine athénienne
- 1.2 L'allégorie

2. Objet et principes

- 2.1 Le problème
- 2.2 Les trois principes de Schumacher
- 2.3 La règle de construction
- 2.4 Le principe de dégradation

3. Topologie : cellules, cercles, fédération

- 3.1 La cellule
- 3.2 Le cercle et le double lien
- 3.3 La délégation liquide est exclue
- 3.4 La fédération
- 3.5 Échelle : 30 millions de personnes

4. Délibération

- 4.1 Les outils
- 4.2 Protocoles de parole
- 4.3 Proposition anonyme
- 4.4 Contradicteur tiré au sort
- 4.5 Rapport de minorité et réexamen

5. Vote

- 5.1 Propriétés visées
- 5.2 Belenios
- 5.3 Les trois rôles humains, séparés dès l'élection test à 10
- 5.4 Fenêtre, quorum, accès
- 5.5 Papier
- 5.6 Revue citoyenne avant vote

6. Voix (VoIP)

- 6.1 Modèle de menace
- 6.2 Briques
- 6.3 Appels de groupe

7. Instabilité du pouvoir : les règles anti-ego

8. Contre le suivisme

9. Ostracisme

10. Mobilité, anti-bot, IA

- 10.1 Mobilité entre cellules
- 10.2 Le système est interdit aux comptes non humains
- 10.3 IA : prévenir les déviations en amont

11. Le fichier de règles et le protocole commun

- 11.1 Principe
- 11.2 Exemple
- 11.3 Bornes du protocole commun

12. Le service de gouvernance et ses invariants

- 12.1 Rôle
- 12.2 Invariants testés par propriétés

13. Infrastructure

- 13.1 Briques déployées telles quelles
- 13.2 Le code écrit (Rust, colle uniquement)
- 13.3 Le nœud dans la cellule
- 13.4 Ce que la cryptographie ne règle pas
- 13.5 Claude et les assistants de code dans la boucle
- 13.4 Le journal : témoins, époques, registre

14. Ordre de marche

15. Décisions actées et historique des révisions

- 15.1 Décisions fermées (19/09/2026)
- 15.2 Corrections issues des relectures adversariales
- 15.3 Écartés en connaissance de cause

Annexe — Sources d'inspiration

*Klérotèrion est un système de démocratie directe horizontale et fédérée, organisé en petites cellules à l'échelle humaine (E.F. Schumacher, *Small is Beautiful*), assemblé à partir de briques libres existantes et auditées, avec des règles explicites contre la concentration du pouvoir, contre le suivisme, contre les bots et contre les dérives de l'IA. Il intègre les cinq décisions actées, les corrections des cinq passes de relecture adversariale et les verdicts du tribunal jusqu'à la v14 (époques du journal, registre papier comme racine de confiance).*

1. Le nom : Klérotèrion

1.1 La machine athénienne

Le *klérotèrion* (κληρωτήριον) est la machine à tirer au sort des Athéniens du IV^e siècle avant notre ère. C'est une dalle de pierre dressée, creusée de colonnes de fentes. Chaque citoyen candidat y glisse son *pinakion*, une petite plaque de bronze gravée à son nom, dans la colonne de sa tribu. Sur le côté, un tube vertical reçoit des boules de bronze, blanches et noires, mélangées. Le magistrat tourne une manivelle : une boule tombe pour chaque rangée de plaques. Boule blanche, la rangée entière est tirée ; boule noire, elle rentre chez elle. Le tirage se fait sur l'agora, devant tout le monde, et personne, pas même le magistrat, ne peut choisir qui sort. Deux exemplaires ont été retrouvés près de l'Agora d'Athènes ; on en voit un au musée de la Stoa d'Attale.

1.2 L'allégorie

Le nom a été choisi parce que chaque pièce de la machine correspond à une pièce du système :

La machine athénienne	Klérotèrion
Le pinakion, plaque de bronze au nom du citoyen, remise par la cité	La clé matérielle FIDO2, remise en main propre par la cellule ; sans plaque, pas de tirage
Les fentes, une par citoyen, une colonne par tribu	Les identifiants de rôle et de vote ; une cellule par personne
Les boules blanches et noires, mélangées hors de portée du magistrat	La balise aléatoire vérifiable, engagée puis révélée : personne ne choisit qui sort
La manivelle tournée en public sur l'agora	Le journal de transparence : chaque tirage est écrit là où tout le monde peut le lire
La dalle de pierre, lisible d'un coup d'oeil, sans mécanisme caché	Le fichier de règles d'une page, et la règle de construction : rien de caché, rien de réécrit
Le tirage qui remplace l'élection	Le tirage au sort de tous les rôles : personne ne fait campagne

L'allégorie dit aussi ce que le système n'est pas. La machine ne gouverne pas : elle désigne qui va servir un temps court, puis on la retourne. Elle n'a pas d'opinion, pas de mémoire, pas de favori. Klérotèrion est une machine à distribuer le pouvoir, pas à l'exercer. Dans l'application, ce nom désigne l'ensemble ; le service de tirage au sort à l'intérieur en est le coeur et porte le même nom.

2. Objet et principes

2.1 Le problème

Mettre 100 000 personnes dans une même assemblée ne produit ni délibération ni décision. La « cacophonie du nombre » n'est pas un problème technique, c'est un problème de topologie. Par ailleurs, un groupe horizontal sans règles explicites ne devient pas égalitaire : il produit une élite invisible et une masse qui suit (Jo Freeman, *La Tyrannie de l'absence de structure*, 1972). Les égos surdimensionnés et le pantouflage des suiveurs sont un seul problème : l'absence de mécanismes qui redistribuent la parole, la charge et la responsabilité.

2.2 Les trois principes de Schumacher

- **Échelle humaine** : au-delà d'une certaine taille, une organisation cesse d'être intelligible pour ses membres.
- **Subsidiarité** : une décision se prend au niveau le plus bas capable de la porter. Le cercle supérieur ne peut pas forcer la cellule sur ce qui relève d'elle.
- **Technologie appropriée** : l'outil doit rester compréhensible et réparable par ceux qui l'utilisent. Une règle qu'on ne peut pas lire n'existe pas.

2.3 La règle de construction

La sécurité vient de ce qu'on n'écrit pas. Tout protocole cryptographique nécessaire existe déjà, audité, parfois formellement vérifié. Le travail est de l'assemblage dans un flake NixOS, pas du développement de primitives. Les briques (Belenios, Loomio, Pol.is, Linphone, ZRTP) sont emballées, fédérées, jamais modifiées.

2.4 Le principe de dégradation

Le système dégrade dans un ordre fixé : la vidéo tombe, puis la voix, puis le confort de délibération, et le vote reste le dernier debout. Le numérique délibère ; pour les décisions à fort enjeu, le papier peut trancher.

3. Topologie : cellules, cercles, fédération

3.1 La cellule

- **Effectif : 20 à 150 membres.** 20 est un plancher arithmétique (assez de personnes pour que les rôles tirés au sort tournent, que les dépositaires, l'autorité d'identifiants et l'administrateur soient distincts, que le quorum ait un sens). 150 est le nombre de Dunbar : au-delà, on ne connaît plus tout le monde et les mécanismes de nivellement cessent de fonctionner.
- **En dessous de 20 :** statut « en formation ». La cellule fonctionne avec toute son autonomie, sans liaison au cercle. Un cercle ne peut jamais imposer une fusion.
- **Au-dessus de 150 :** scission en deux, par tirage au sort des membres si la cellule ne s'entend pas sur la ligne de partage.
- **Groupes de travail** (5 à 15 membres) : délibèrent sur un sujet ; la cellule vote.
- C'est le seul niveau où tout le monde parle et vote sur tout.

3.2 Le cercle et le double lien

Chaque cellule envoie deux représentants au cercle supérieur : l'un désigné par la cellule, l'autre par le cercle du dessus (double lien sociocratique). Ils sont révocables à tout moment. Ce n'est pas une délégation de pouvoir, c'est une délégation de voix, et c'est **la seule délégation du système**, publique par nature. Les représentants siègent avec un identifiant de rôle expirant, pas leur identité de membre. Jamais une seule personne sur un lien (co-présidence).

3.3 La délégation liquide est exclue

Décision actée, définitive : pas de délégation liquide, sous aucune forme. Une table de délégations révèle qui suit qui, ce qui est incompatible avec le vote secret et avec l'invariant « le service ne connaît aucun vote individuel ». Le précédent de LiquidFeedback (super-électeurs, effondrement de la participation) confirme le choix.

3.4 La fédération

Pas d'instance commune. Les échanges entre cellules sont **tolérants au délai** : des faits signés (décomptes, tirages, mandats) relayés quand la liaison existe, jamais du contenu. Une cellule coupée plusieurs jours reste valide et se resynchronise.

3.5 Échelle : 30 millions de personnes

Niveau	Unités	Échelle
1	300 000 cellules	quartier, village, coopérative
2	30 000	commune
3	3 000	canton
4	300	département
5	30	région
6	3	pays

Six niveaux, chaque cercle restant une assemblée de 20 personnes. Ce qui change vraiment d'échelle, c'est le **nombre de décisions par niveau** : chaque niveau a un plafond de questions

ouvertes, et une question ne monte que si un cercle du niveau inférieur la fait monter par consentement.

- **Référendum fédéré** : aucun serveur de vote national. Chaque cellule tient son scrutin Belenios sur la même question et publie son décompte vérifié ; le résultat national est la somme de 300 000 décomptes agrégés dans un arbre de Merkle d'arbres de Merkle.
- **Assemblée tirée au sort** : 1 000 personnes stratifiées (représentatives à $\pm 3\%$) préparent la question ; le pays vote ensuite par référendum fédéré.
- **Pol.is en niveaux** : une conversation par cercle de niveau 3, dont les points de consensus alimentent le niveau supérieur.
- **Mandats exécutifs** pour l'urgence : petit cercle tiré au sort, mandat court, décisions immédiates mais révisables.
- **Séparation des fonctions** (Bouricius) aux niveaux 3 et plus : agenda, rédaction, révision, décision, contrôle, par cinq corps tirés au sort distincts.
- **Statut de ces mécanismes** : panel citoyen, cinq corps, seconde lecture, niveaux 2 et 3 sont **non normatifs** tant qu'ils ne sont pas spécifiés (délais, règles d'échec) et éprouvés par une fédération réelle. On ne construit pas pour 30 millions ; on documente l'intention.
- **Unicité des personnes** : en v1, la cellule garantit elle-même ses membres. L'attestation aveugle par une identité d'État est une v3, au-delà de cent cellules. Une fausse déclaration de première adhésion reste une hypothèse de confiance jusque-là.

4. Délibération

4.1 Les outils

- **Pol.is** (AGPL) : chacun propose des affirmations courtes, tout le monde vote d'accord ou pas d'accord ; une réduction de dimension dessine les groupes d'opinion et les points de consensus transversaux. Pas de réponse aux réponses, pas de likes, pas de followers. Utilisé par vTaiwan depuis 2015.
- **Loomio** (AGPL, Ruby/Vue) : propositions, amendements, vote par consentement (une proposition passe si personne n'a d'objection argumentée), échéances, délibération asynchrone.
- **Tirage au sort** pour les comités de rédaction, à la manière des assemblées citoyennes.

4.2 Protocoles de parole

Règle	Origine
Les moins anciens dans la cellule parlent d'abord	Règle de saint Benoît (ch. 3), pile progressive
Le coordinateur parle en dernier et synthétise	Kgotla tswana
Silence entre les prises de parole ; on répond à la question, jamais à une personne	Quakers, tours sociocratiques
Un secrétaire (clerc) formule le sens de l'assemblée	Quakers
Temps de parole égal, non cumulable ; aucune métrique de réputation persistante	Pol.is, Occupy
Pré-mortem avant toute décision à fort enjeu	Gary Klein

4.3 Proposition anonyme

Chaque membre reçoit un lot fixe de jetons RSA aveugles par mois (par exemple 3), en une fois, qu'il s'en serve ou non : le moment d'obtention ne trahit rien et le lot borne les propositions en rafale. L'auteur dépose via un relais oignon auprès du **point de dépôt** du service de gouvernance, qui vérifie le jeton et publie dans Loomio sous un compte technique partagé. L'auteur publie un engagement $H(\text{proposition} \parallel \text{id_auteur} \parallel \text{nonce})$ et l'ouvre après le vote s'il le souhaite, ou jamais. Limite connue : le contradicteur tiré au sort peut être l'auteur lui-même.

4.4 Contradicteur tiré au sort

À l'ouverture d'une proposition, un membre est tiré et notifié ; il doit porter la meilleure objection possible, même s'il est d'accord. Délai de 72 h, sinon nouveau tirage, trois tirages au maximum, puis clôture autorisée avec mention « aucune objection reçue » au journal.

4.5 Rapport de minorité et réexamen

Les clusters minoritaires de Pol.is sont joints automatiquement au compte rendu. Toute décision adoptée crée une proposition de réexamen à date fixe (un an par défaut) ; au-delà du niveau 2, seconde lecture obligatoire. Quand une décision réexaminée est jugée nuisible, le journal le note **sur la décision, jamais sur une personne** (graphè paranomôn, version douce corrigée en v9).

5. Vote

5.1 Propriétés visées

- **Éligibilité** : seuls les membres votent, une seule fois.
- **Secret** : personne, pas même l'infrastructure, ne peut relier un bulletin à une personne.
- **Vérifiabilité de bout en bout** : chaque votant vérifie que son bulletin est enregistré ; n'importe qui vérifie que le décompte est juste.
- **Absence de reçu** : nul ne peut prouver à un tiers comment il a voté.

5.2 Belenios

Belenios (Inria/CNRS/LORIA) : chiffrement ElGamal homomorphe, les bulletins s'additionnent chiffrés et seul le total est déchiffré ; chaque bulletin porte une preuve à divulgation nulle qu'il est bien formé ; les bulletins vont sur un tableau d'affichage public append-only. Protocole vérifié en ProVerif. On l'emballa, on ne le modifie pas.

5.3 Les trois rôles humains, séparés dès l'élection test à 10

Rôle	Qui	Ce qu'il protège
Administrateur du nœud	Membre en charge du serveur de la cellule	Le fonctionnement
Autorité d'identifiants	Membre tiré au sort pour chaque scrutin, sur sa machine, avec l'outil Belenios ; travaille avec la liste nominative ; jamais l'administrateur	Contre l'ajout de bulletins (collusion avec le serveur)
Autorités de déchiffrement (détenteurs de parts)	7 membres tirés au sort pour chaque scrutin, seuil 4 sur 7, clé matérielle chacun ; jamais l'administrateur ni l'autorité d'identifiants du même scrutin	Le secret du vote

Les trois rôles sont disjoints : 9 personnes au minimum, d'où une genèse de cellule à **10 fondateurs**. Les rôles à plusieurs sièges (détenteurs, témoins du journal, gardiens) tournent par **rotation équitable** (décision 13) : les places vont d'abord aux moins servis sur cinq ans, et deux mandats de suite sont interdits dès que les éligibles sont au moins deux fois plus nombreux que les sièges. La règle stricte « deux par rôle par cinq ans » ne vaut que pour les rôles à siège unique : appliquée aux sept détenteurs, elle exigerait 60 membres.

Les électeurs vérifient que le nombre d'identifiants publiés correspond à l'effectif. Le vote final se fait **sans débat interne** : la délibération précède, le vote ne discute plus (Policy Jury de Bouricius).

5.4 Fenêtre, quorum, accès

- **Fenêtre de vote fixée à l'ouverture, 96 h** (décision 14). Aucune date de scrutin ne change jamais après l'ouverture : un déclencheur de prolongation était une surface de manipulation (une coalition de 10 % pouvait l'activer sans panne), une durée fixe n'en a aucune.
- **Quorum de participation** : une décision n'est valide que si une part suffisante de la cellule a voté, pas seulement des présents. L'abstention de masse invalide.
- **Les métriques d'accès** (bulletins par heure, échecs de connexion) sont versées au journal, agrégées, jamais nominatives. Elles servent de preuve, elles ne pilotent plus rien.

- Terminal partagé sur le réseau local de la cellule pour ceux dont la liaison ne suit pas ; il sert aussi contre la coercition à domicile.

5.5 Papier

Décision actée : bulletin papier de secours pour les décisions à fort enjeu. Le numérique délibère, le papier peut trancher.

5.6 Revue citoyenne avant vote

Pour toute décision à fort enjeu, un panel de 5 membres tirés au sort produit une page pro/contre versée au scrutin avant son ouverture (modèle Oregon Citizens' Initiative Review, dont les évaluations montrent un gain mesurable de connaissance des votants).

6. Voix (VoIP)

6.1 Modèle de menace

Trois choses à protéger, par difficulté croissante : le contenu (chiffrement de bout en bout), l'authenticité (savoir à qui l'on parle), les métadonnées (qui appelle qui, quand).

6.2 Briques

- **Linphone + Flexisip** (GPL, Grenoble) : client SIP, serveur auto-hébergé par cellule. Décision actée : Linphone seul, pas de Matrix.
- **ZRTP hybride post-quantique** : échange de clés dans le flux média, sans PKI, avec **SAS** (deux mots affichés, lus à voix haute par les deux interlocuteurs ; s'ils diffèrent, il y a un intermédiaire). Continuité de clés d'un appel à l'autre.
- **Opus en débit constant (CBR)** à 24 kbit/s, avec padding : le débit variable fuit des phrases entières dans un flux chiffré.
- **coturn** local : relais des flux chiffrés entre deux membres de la même cellule.
- Signalisation via relais oignon ; aucun numéro de téléphone, aucune passerelle vers le réseau téléphonique.

6.3 Appels de groupe

Phase 1 : conférences Linphone (bout en bout via LIME, à **vérifier** avant de s'y fier). Phase ultérieure : **SFrame sur MLS** via Soley, qui implémente déjà MLS RFC 9420, Kyber-768 et Dilithium3. Une seule voie par phase. Règle en vigueur jusque-là : le SAS n'authentifie que le serveur dans une conférence, donc **aucune décision à fort enjeu ne se prend sur la foi d'un appel de groupe**. Audio seul par défaut, vidéo optionnelle.

7. Instabilité du pouvoir : les règles anti-ego

Règle	Détail	Origine
Tirage au sort	Tous les rôles de coordination, rédaction, représentation ; balise aléatoire vérifiable (tirage engagé puis révélé au journal)	Athènes
Mandats courts, rotation	3 à 6 mois ; identifiant de rôle qui expire à date fixe, sans chemin de code pour prolonger	Athènes, Zapatistes
Non-cumul relatif	Rôles à siège unique : pas deux mandats consécutifs, pas plus de deux par période de cinq ans. Rôles à plusieurs sièges : rotation équitable (§5.3)	Boulè, adapté à la petite échelle
Révocabilité	À tout moment, majorité simple, sans motif ; le corps qui révoque (la cellule) n'est jamais le corps qui exécute	Haudenosaunee
Euthyna	Audit obligatoire de fin de mandat pour tout rôle clé, publié au journal ; l'ostracisme peut suivre	Athènes
Alternance sort / vote	Désignations sensibles au niveau 3 et plus : tirage d'un panel, qui vote, réduit par le sort	Venise, 1268
Consentement, pas majorité	Une objection doit être argumentée et vérifiable	Sociocratie
Plafond de ressources	Si la fédération gère des ressources : écart 1:5 maximum	Mondragón

8. Contre le suivisme

- **Vote secret systématique**, y compris en cellule : la conformité s'effondre quand on ne voit pas les autres (Asch). Le chiffrement du vote est un outil contre le grégarisme.
- **Rôles tournants pour tout le monde** : chacun tient à son tour secrétariat, rapport, contradiction.
- **Contradicteur tiré au sort** par décision (§4.4).
- **Rapport de minorité** obligatoire ; **révision à échéance** ; **participation comme quorum**.
- **Conditions de Condorcet / Surowiecki** : une foule n'est sage que si ses membres sont indépendants, divers, décentralisés et proprement agrégés. Le vote secret et l'absence de réponses aux réponses en sont l'application ; la cacophonie détruit l'indépendance.

9. Ostracisme

Distinct de la révocation, qui retire un mandat en cours : l'ostracisme rend une **personne** inéligible aux rôles clés, à titre préventif, sans procès ni motif à prouver. Les trois cas qui le justifient (pouvoir pour soi, corruption, abus de position) sont la doctrine de l'outil, pas des chefs d'accusation.

- **Portée** : rôles clés seulement (coordination, liaison, exécutif, autorité d'identifiants, dépositaire).
- **Effet** : inéligibilité à tout rôle clé pour une durée fixe (deux ans par défaut), à tous les niveaux ; rien d'autre. La personne vote, délibère, propose.
- **Déclenchement** : initiative citoyenne anonyme (seuil de membres, jetons aveugles du lot mensuel). Les rôles clés en exercice ne peuvent pas signer (contre la collusion de type Hyperbolos, 417 av. J.-C., qui a tué l'institution athénienne).
- **Deux votes secrets dans l'ordre** : d'abord « faut-il ouvrir un ostracisme ce cycle ? » sans nom, puis seulement le nom. Quorum renforcé (deux tiers de participation). Un par cellule et par an.
- **Droit de réponse écrit** de 72 h au journal avant le second vote.
- L'inéligibilité **suit la personne** dans toute la fédération, via l'attestation de départ.

10. Mobilité, anti-bot, IA

10.1 Mobilité entre cellules

- Une personne, une cellule à la fois. Départ libre pour motif d'affinité ou d'efficacité, sans justification.
- **Pas de départ pendant un engagement** : scrutin ouvert où la personne a reçu un identifiant, mandat en cours, procédure d'ostracisme la visant. Cela empêche de fuir un ostracisme, de voter deux fois, ou de bourrer une cellule.
- Carence de 30 jours après l'arrivée avant de voter ; deux changements par an au maximum.
- Entrée sur accueil par la cellule d'arrivée (deux parrains), qui exige une **attestation de départ** de la cellule d'origine. L'attestation transporte la date de fin d'inéligibilité et le compteur de mandats, jamais les votes.

10.2 Le système est interdit aux comptes non humains

Pas de CAPTCHA, pas de biométrie, pas de score de confiance. La preuve d'humanité est physique :

- La clé matérielle FIDO2 est remise **en main propre**, lors d'une réunion de cellule, en présence de deux parrains. Sans clé matérielle : pas de jeton, pas d'identifiant, pas de dépôt, pas d'appel.
- Aucune API d'écriture ouverte ; tout passe par le point de dépôt avec un jeton du lot mensuel, qui est une limite de débit par humain.
- Les comptes techniques (publication anonyme, action du service de gouvernance sur Loomio) et les clés de service (journal, émission de jetons) existent ; l'invariant vise les **accréditations de membre** : clé FIDO2, jeton, identifiant de vote. Aucune n'est jamais détenue par un compte non humain.
- Il n'existe aucun chemin de code pour créer une accréditation sans clé remise en personne.

10.3 IA : prévenir les déviations en amont

1. **L'IA n'est jamais un participant.** Ni clé, ni jeton, ni identifiant ; elle ne propose, ne vote, ne signe, ne délègue, ne délibère. Invariant codé.
2. **L'IA est un outil sous le nom d'un humain**, pour des usages énumérés : résumé, traduction, accessibilité, aide à la rédaction. Le marquage au journal est garanti pour l'outil de la cellule, déclaratif ailleurs (indétectable sur la machine d'un membre). Le membre reste responsable de ce qu'il dépose.
3. **Modèles locaux uniquement**, dans une cage séparée, sans accès au journal ni au coffre. Aucun hyperscaler dans la boucle d'une décision. Le service de gouvernance ne contient aucun modèle. Le clustering de Pol.is est libre, déterministe à graine fixée et inscrite au journal, rejouable par quiconque.
4. **Le vrai risque est l'humain augmenté** (une personne, des dizaines de propositions calibrées). Parades : lot mensuel (volume), engagement d'auteur (paternité), contradicteur humain, vote secret sans débat.
5. **Voix** : vérification SAS à deux ; pas de décision à fort enjeu en conférence tant que le bout en bout n'est pas en place.
6. La section [ia] du fichier de règles expire au bout d'un an et doit être relue par la cellule, avec pré-mortem.

11. Le fichier de règles et le protocole commun

11.1 Principe

Les règles ne sont pas dans la plateforme mais dans un **fichier TOML par cellule**, en clair, lisible en deux minutes, signé par la cellule, modifiable uniquement par un vote Belenios de la cellule. Le cercle supérieur peut le lire, jamais le modifier ; il vérifie seulement le respect de bornes minimales.

11.2 Exemple

```
[cellule]
nom = "Le Marin – quartier du port"
effectif_max = 150

[mandats]
duree_jours = 120
consecutifs_interdits = true
max_par_role_sur_5_ans = 2
roles = ["coordination", "secretariat", "liaison-cercle"]

[vote]
quorum_participation = 0.5
secret = true
fenetre_heures = 96
papier_si_enjeu_fort = true
dechiffrement_seuil = 4
dechiffrement_detenteurs = 7
rotation_sieges_multiples = "equitable"

[journal]
temoins = 6
quorum = 4
epoque = "mandat"
renouvellement_hors_scrutin = true

[registre]
exemplaires = 2
gardiens = 2

[propositions]
jetons_par_mois = 3

[deliberation]
proposition_anonyme = true
contradicteur_tire_au_sort = true
contradicteur_delai_heures = 72
contradicteur_tirages_max = 3
reexamen_jours = 365

[ostracisme]
roles_cles = ["coordination", "liaison-cercle", "executif", "autorite-identifiants",
"depositaire"]
seuil_initiative = 0.10
quorum_participation = 0.66
duree_ineligibilite_jours = 730
reponse_delai_heures = 72
max_par_an = 1
```

```

[membres]
effectif_min = 20
effectif_max = 150
parrains_requis = 2
remise_cle_en_personne = true
carence_apres_arrivee_jours = 30
changements_par_an_max = 2

[ia]
participant = false
usages_autorises = ["resume", "traduction", "accessibilite", "aide-redaction"]
marquage_journal = true
modeles_locaux_uniquement = true
expiration = "2027-09-19"

```

11.3 Bornes du protocole commun

secret = true obligatoire ; dechiffrement_seuil ≥ 4 sur 7 ; fenetre_heures = 96 fixe ;
journal:temoins = 6, quorum = 4 ($2q - n \geq 2$ et $q > n/2$ pour tout ensemble en vigueur) ;
registre:exemplaires = 2 ; duree_jours ≤ 180 ; quorum_participation ≥ 0.3 ;
ostracisme:max_par_an ≤ 1 , duree_ineligibilite_jours ≤ 1095 ,
reponse_delai_heures ≥ 72 ; membres:20 $\leq$ effectif ≤ 150 ,
remise_cle_en_personne = true ; IA:participant = false, modeles_locaux_uniquement
= true.

12. Le service de gouvernance et ses invariants

12.1 Rôle

La seule pièce de code contenant de la logique politique. Petite par construction : une machine à états déterministe, sans modèle statistique.

- **Entrée** : le fichier de règles, les événements Loomio, les décomptes Belenios, l'annuaire du service d'identité.
- **Sortie** : des faits datés et signés dans le journal de transparence (tirage effectué, mandat expiré, quorum non atteint, contradicteur désigné, fenêtre prolongée, métriques d'accès agrégées), et des actions via l'API Loomio (proposition de réexamen, rapport de minorité, notification du contradicteur, publication anonyme).
- **Interdits** : lire un bulletin, connaître un vote individuel, modifier une règle. Le service refuse de démarrer si la signature du fichier de règles ne correspond pas.

12.2 Invariants testés par propriétés

- Un mandat ne dépasse jamais sa durée ; pas deux mandats consécutifs sur un même rôle ; pas plus de deux par rôle par cinq ans.
- Un tirage n'est jamais rejouable.
- Une proposition n'attend jamais plus de 3×72 h son contradicteur.
- L'administrateur du nœud n'est jamais autorité d'identifiants ; aucune autorité de déchiffrement n'est administrateur ni autorité d'identifiants du même scrutin ; le déchiffrement exige toujours le seuil.
- Aucune date de scrutin ne change après l'ouverture.
- Un journal n'a qu'une politique de témoins pour toute sa vie ; une époque ne s'ouvre qu'après clôture cosignée de la précédente et inscription au registre ; deux quorums de témoins ne peuvent jamais être disjoints ; un témoin ne cosigne qu'une tête qui prolonge sa dernière signature.
- Le quorum de témoins ne se démontre pas, il se calcule : $2q - n \geq f + 1$ avec $f = 1$.
- Un ostracisé n'est jamais tiré pour un rôle clé avant sa date et garde tous ses droits de membre ; un rôle clé en exercice ne signe jamais une initiative d'ostracisme ; jamais plus d'un ostracisme par cellule et par an ; le vote nominal n'a jamais lieu sans le vote de principe.
- Une personne n'est membre que d'une cellule à la fois (garanti pour les départs attestés) ; un membre engagé ne quitte jamais sa cellule ; une inéligibilité suit la personne.
- Aucune accréditation de membre n'existe sans clé matérielle remise en personne ; aucune n'est détenue par un compte non humain.

13. Infrastructure

13.1 Briques déployées telles quelles

Couche	Brique	Phase 1
Délibération	Pol.is, Loomio	Conteneur OCI fixé par empreinte, reverse proxy, OIDC
Vote	Belenios	Conteneur OCI fixé par empreinte
Voix	Linphone + Flexisip	Conteneur OCI, ZRTP PQ, Opus CBR
Relais	coturn	Conteneur OCI
Supervision	Prometheus + Grafana, exporters standard	Conteneur OCI

Aucune de ces briques n'a de module NixOS prêt. Phase 1 : images OCI existantes fixées par empreinte (image@sha256:..., jamais par étiquette), dans `virtualisation.oci-containers`. En phase 1, la cellule voisine vérifie qu'elle fait tourner une image identique, **pas** qu'elle a reconstruit le logiciel depuis ses sources ; la reconstruction au bit près vient avec le packaging Nix natif.

13.2 Le code écrit (Rust, colle uniquement)

- **Service d'identité** : lots mensuels de jetons RSA aveugles (RFC 9474), passerelle OIDC, carnet SIP. Ne tient pas le rôle d'autorité d'identifiants Belenios (§5.3). Colle cryptographique : Lane 2 (local).
- **Journal de transparence** : arbre de Merkle append-only (RFC 6962), avec le protocole de témoins existant, voir §13.4. Aucun code de consensus.
- **Service de gouvernance** (§12).
- **Distribution des clés SFrame** via le groupe MLS de Soley, `sframe-rs`, `str0m` (phase ultérieure).

Aucune primitive cryptographique n'est écrite. `#![forbid(unsafe_code)]`, `proptest`, `cargo-fuzz` sur tout ce qui parse, `cargo-deny`, `cargo-audit`, builds reproductibles publiés avec leur hash.

13.3 Le nœud dans la cellule

Chaque cellule héberge son nœud sur son réseau local, sur du matériel modeste. Un membre sur place l'atteint sans passer par Internet. Pas de datacenter : la capacité totale est celle des cellules. Une panne touche une cellule, jamais le pays.

13.4 Ce que la cryptographie ne règle pas

- **La coercition physique** : revote possible (le dernier bulletin compte), terminal partagé en cellule.
- **Le terminal du votant** : maillon faible de tous les systèmes (Estonie, Suisse/Scytl 2019). D'où le terminal dédié minimal et le papier de secours.
- **La capture sociale** : tirage au sort, révocabilité, rotation, ostracisme. Ostrom : ce qui tient, ce sont des règles écrites par ceux qui les subissent, une surveillance mutuelle, des sanctions graduées et une résolution des conflits bon marché.

13.5 Claude et les assistants de code dans la boucle

Un modèle hébergé aux États-Unis est une dépendance à traiter comme les autres. Pertinent pour les modules Nix, la colle, les tests, la CI, la génération de tests adversariaux, la relecture comme plaideur (jamais juge unique), la rédaction. Exclu de la distribution des clés et de tout ce qui touche Soley (Lane 2), des secrets, et de tout mode sans permissions sur un nœud de cellule. Rien de ce qu'il écrit n'entre en production sans tribunal et CI ; rien de secret n'entre dans son contexte. Le test : le flake se rebuild à l'identique sans lui.

13.4 Le journal : témoins, époques, registre

La règle du §4 : aucun protocole de consensus maison. Si un besoin semble exiger un protocole d'accord écrit par nous, on cherche d'abord la brique qui le résout ; si elle ne le résout pas, on n'écrit pas la surcouche : le journal s'arrête, l'assemblée tranche, le papier prend le relais. Trois versions de la spécification (v10 à v12) ont été rejetées pour avoir violé cette règle en la croyant respectée.

La brique. Le protocole de témoins des journaux de transparence : C2SP **tlog-witness** v1.0.0 (un témoin garde le dernier point de contrôle vérifié, n'accepte la suite que sur preuve de cohérence, refuse par 409 une branche concurrente), **tlog-cosignature** (Ed25519 ; ML-DSA-44 à vérifier dans le texte de la spécification), **tlog-policy** (le quorum k parmi n , sans paramètre maison). Implémentation : transparency-dev/witness (Go, épinglé par empreinte de commit, go.sum et chaîne de compilation figés via buildGoModule et vendorHash) ou le témoin de Sigsum ; un crate Rust n'est retenu que s'il passe l'examen de maintenance et cargo-deny. La spécification dit elle-même ce qu'elle ne couvre pas : ni l'amorçage d'un témoin sur une tête existante, ni la résolution d'une vue divisée. On ne le lui demande donc pas.

Le quorum. 6 témoins, 4 cosignatures. C'est la plus petite combinaison qui satisfait $2q - n \geq f + 1$ avec un complice (deux quorums se croisent toujours sur un témoin honnête) tout en tolérant deux absents ; 4 sur 3 est le minimum théorique avec un seul absent. La garantie est à **un complice** ; à deux, une vue divisée est possible, et c'est le résidu nommé. Un témoin qui perd son état n'est pas réamorçé : le journal continue à 5 (un absent toléré) jusqu'à l'époque suivante. La clé de témoin est une clé Ed25519 **distincte de la clé FIDO2** (qui ne signe que des assertions WebAuthn) : c'est une accréditation de membre de plus, remise en personne, inscrite à l'inventaire.

Les époques. Un journal, une politique, une époque par mandat. On ne fait jamais de transition de politique dans un journal : la coexistence de deux ensembles de témoins (union à 7, ou 9 lors d'un renouvellement par moitié) recrée exactement la vue divisée. Le renouvellement est une **genèse** : un nouveau journal vide, six témoins neufs (démarrer sur un journal vide est natif dans la brique), dont la première entrée contient la tête finale de l'époque précédente avec ses cosignatures au quorum. Les anciens témoins cessent de signer et détruisent leur clé d'époque (hygiène, pas sécurité : une clé conservée ne cosigne qu'un journal clos). Tant que la clôture n'est pas cosignée et inscrite au registre, la nouvelle époque n'accepte rien. Condition de départ : les témoins concernés présents en assemblée, appareils en main, clés accessibles. Si un second témoin tombe en cours d'époque, l'assemblée peut ouvrir une époque sans attendre la fin du mandat.

Le registre papier, racine de confiance. Deux exemplaires, deux gardiens tirés au sort par mandat, jamais l'administrateur, jamais les gardiens des disques. À chaque tête finale et chaque genèse : lecture à voix haute par deux personnes (l'une lit, l'autre vérifie sur son propre client), recopie à la main dans les deux exemplaires, page signée par tous les présents. On y porte la tête, la genèse, l'empreinte de la politique de l'époque et les incidents. Ce qu'il tranche : la **genèse rivale**. Deux nouveaux journaux qui prétendent succéder à la même tête finale sont tous deux bien formés ; aucune vérification cryptographique ne les départage ; l'époque valide est celle qui figure au registre, et un client refuse une genèse absente. Divergence entre les deux exemplaires : le journal

s'arrête, l'assemblée est convoquée, aucune époque ne s'ouvre tant qu'ils ne concordent pas. Perte des deux : la cellule repart par une genèse déclarée ; l'histoire antérieure reste vérifiable mais plus arbitraire. Le registre ne prouve pas le contenu du journal : il dit quelle histoire la cellule a reconnue comme la sienne. C'est précisément ce que la cryptographie ne peut pas fournir.

Barrière de semaine 4. Trois capacités natives à vérifier sur banc avant tout déploiement : démarrer sur un journal vide, refuser une branche concurrente, exiger un quorum côté client. Si l'une manque : arrêt et retour au tribunal, jamais d'adaptateur.

Hypothèses de confiance déclarées. Copie possible du coffre une fois ouvert ; surémission ou transfert d'un jeton d'initiative ; automatisation d'un compte authentique (le dispositif bloque les faux comptes, pas un membre qui scripte sa propre clé ; le lot mensuel borne le volume).

14. Ordre de marche

1. Flake avec les cinq briques en OCI (semaines 1 à 3). Une cellule test de 10 personnes réelles, en formation, avec un vrai sujet à décider.
2. Service d'identité (jetons, point de dépôt) et journal de transparence (semaines 4 et 5). Rôles humains d'autorité d'identifiants et de dépositaires tirés au sort dès la première élection test.
3. Barrière de semaine 4 sur le journal (§13.4), puis service de gouvernance : fichier de règles, tirage au sort, expiration des mandats (semaines 6 et 7). Un cycle complet de mandat court (30 jours) avec tirage, rotation, révocation et un scrutin à trois rôles.
4. Contradicteur, engagement d'auteur, réexamen, ostracisme, mobilité (semaine 8).
5. SFrame sur MLS via Soley pour les appels de groupe, en remplacement des conférences Linphone.
6. Publication en AGPL sur Codeberg dès la première cellule : un système de vote fermé n'est pas un système de vote.

L'exercice de la cellule test commence par un **changement d'époque** (registre compris), une **division provoquée** du journal, les deux mauvaises façons de renouveler les témoins jouées exprès (à 3 le journal s'arrête, à 9 il se divise seul), puis un scrutin à trois rôles séparés. Trois mesures : le temps réel d'un changement d'époque ; le nombre de refus de rôle tiré au sort et leurs raisons ; ce que font les dix personnes dans les dix minutes suivant le premier arrêt du journal, sans que personne ne souffle la procédure.

Le premier livrable n'est pas le flake : c'est la première cellule. Si dix personnes acceptent d'être tirées au sort, de tenir une clé et de rendre un mandat au bout de trente jours, le reste suit.

15. Décisions actées et historique des révisions

15.1 Décisions fermées (19/09/2026)

1. Unicité des personnes : la cellule garantit ses membres en v1 ; attestation par identité d'État en v3, au-delà de cent cellules.
2. Délégation liquide : supprimée, définitivement.
3. Voix : Linphone seul jusqu'à ce que Soley porte SFrame ; pas de Matrix.
4. Belenios : les trois rôles humains séparés dès la première élection test, même à 10.
5. Papier : bulletin de secours pour les décisions à fort enjeu.
6. (Décision 13) Rotation équitable pour les rôles à plusieurs sièges.
7. (Décision 14) Fenêtre de vote fixe de 96 h, sans déclencheur de prolongation.

15.2 Corrections issues des relectures adversariales

- Proposition anonyme : engagement ouvert par l'auteur seul, jetons en lot mensuel, point de dépôt, relais oignon.
- Délégation liquide supprimée ; double lien comme seule délégation.
- Contradicteur : 72 h, trois tirages, clôture.
- Autorité d'identifiants : rôle humain tiré au sort, jamais l'administrateur ; liste nominative.
- Autorités de déchiffrement : seuil 3/5, exclusions croisées.
- OCI par empreinte ; honnêteté sur ce qui est vérifié en phase 1.
- Fichier de règles lisible par le cercle, non modifiable.
- Element Call et LiveKit retirés ; une voie par phase.
- Supervision, métriques d'accès, fenêtre de 72 h et prolongation automatique.
- Ostracisme, avec droit de réponse et interdiction de signer pour les rôles en exercice.
- v10 à v14 (tribunal Fugu) : finalisation du journal par quorum et non par délai ; retrait de la surcouche de consensus maison ; brique tlog-witness nommée et versionnée ; 6 témoins, 4 signatures, clé Ed25519 distincte ; amorçage au quorum et non à deux signatures ; interdiction de toute transition de politique dans un journal (union de deux ensembles = vue divisée) ; époques par mandat avec genèse cosignée ; registre papier comme racine de confiance ; genèse à 10 fondateurs ; scission et fusion en machines à états ; mécanismes de la Partie III marqués non normatifs ; hypothèses de confiance déclarées ; scripts de simulation et empreintes en annexe.
- v9 : note de nuisance sur la décision, pas sur la personne ; non-cumul relatif (deux par rôle par cinq ans, jamais consécutifs) ; attestation de départ ; statut « en formation » ; invariant anti-bot recentré sur les accréditations de membre ; marquage IA garanti sur l'outil de cellule, déclaratif ailleurs, modèles en cage ; SAS inopérant en conférence.

15.3 Écartés en connaissance de cause

Démocratie liquide ; consensus strict (liberum veto) ; minipublics purement consultatifs (Convention climat, Islande 2012) ; épistocratie ; futarchie ; blockchain (règle un problème que la démocratie n'a pas et en crée d'autres).

Annexe — Sources d'inspiration

Mécanisme	Origine	Protège contre
Hiérarchie de dominance inversée	Chasseurs-cueilleurs (Boehm)	Émergence d'un dominant
Insulter la viande	!Kung (Lee)	Prestige converti en pouvoir
Kgotla	Tswana	Confiscation de la parole
Sens de l'assemblée	Quakers	Majorité brute, emballement
Les plus jeunes d'abord	Règle de saint Benoît	Déférence hiérarchique
Ostracisme, dokimasia, euthyna, graphè paranomôn, Boulè	Athènes	Tyrannie, démagogie, capture des charges
Élection du doge	Venise 1268	Noyautage par factions
Collégialité, veto	Rome	Monopole exécutif
Mères de clan	Haudenosaunee	Chef non responsable
Mandar obedeciendo, rotation	Zapatistes	Culte du chef
Co-présidence, quotas	Rojava	Monopole du pouvoir
Une voix, plafond salarial	Mondragón	Pouvoir économique converti en politique
Sortition multi-corps	Bouricius	Accumulation dans un seul corps
Revue citoyenne	Oregon	Vote mal informé
Conseil citoyen permanent	Ostbelgien	Court-termisme
Pol.is	vTaiwan	Voix bruyantes, polarisation
Sondage délibératif	Fishkin	Opinion non informée
Pré-mortem	Klein	Pensée de groupe