Architecture Sovereign-Record pour les plateformes à l'échelle communautaire

John G. Stroh

Document A · Projet de révision v4, mai 2026 | Langues : EN · DE · MI

Lire le HTML Télécharger le PDF Voir le diaporama Envoyer des commentaires

Les commentaires de fond portant sur des sections spécifiques sont les bienvenus. Veuillez citer les numéros de section (par exemple §6.10) afin que les corrections puissent être retracées. L'auteur répond personnellement ; veuillez prévoir un délai d'une à deux semaines. L'article est disponible en anglais, en te reo Māori et en allemand (liens ci-dessus). Le diaporama est actuellement disponible uniquement en anglais ; des diaporamas localisés suivront lors de la version candidate de la v4.

Architecture de registres souverains pour les plateformes à l'échelle communautaire Plateformes

Provenance cryptographique, application des politiques limitées aux locataires, fédération bilatérale et portabilité souveraine pilotée par les membres pour les infrastructures communautaires non hyperscalers

John G. Stroh

03/05/2026

Sovereign-Record Architecture pour les plateformes à l'échelle communautaire

Résumé

La plateforme communautaire par défaut appartient à une société américaine, est hébergée sur une infrastructure contrôlée par les États-Unis, est monétisée par l’extraction d’attention et est régie par des conditions que l’opérateur peut modifier unilatéralement. L'omniprésence de cette norme par défaut n'est pas le fruit d'un accord fondé sur des valeurs communes convenu par des communautés ayant pesé le pour et le contre ; c'est la conséquence de plus d' une décennie d'investissements soutenus de la part des entreprises pour façonner les attentes des utilisateurs, mettre en place des mécanismes de verrouillage par effet de réseau et orienter le discours public de manière à rendre les alternatives impraticables ou invisibles. Ces conditions persistent sans relâche, indépendamment du consentement de la communauté, et ne se manifestent par des défaillances visibles que de manière intermittente — un compte verrouillé, une publication supprimée, un service fermé sans préavis, une révision des conditions d’utilisation contraire à l’intérêt de la communauté. Pour certaines communautés — les communautés maories détentrices de taonga, les communautés de langues minoritaires dont le contenu *est* la langue elle-même, les groupes d’histoire familiale détenant des archives sur des personnes vivantes identifiées, et toute communauté dont le mode de vie ne se réduit pas à un profil — ces conditions ne sont pas des inconvénients supportables ; ce sont des obstacles structurels au travail pour lequel la communauté existe. Cet article présente une **architecture de documents souverains** — un substrat alternatif dans lequel les propriétés de souveraineté dont une communauté a besoin sont inhérentes aux documents eux-mêmes, et non des concessions que l’opérateur pourrait révoquer.

Chaque enregistrement de contenu du système porte sa propre provenance, sa propre politique d’accès, son propre identifiant de chiffrement et une chaîne cryptographique de toutes les frontières de gouvernance qu’il a franchies. Les lectures exposent cet état aux consommateurs ; les écritures y ajoutent des éléments ; les suppressions le

marquent comme obsolète. La fédération entre locataires souverains est bilatérale et délimitée : deux communautés s’accordent, selon des conditions qu’elles spécifient, sur une interaction spécifique, et uniquement celle-ci. Les membres sont des personnes concernées de premier rang, quel que soit le cadre réglementaire qui leur est applicable : chacun peut exporter l’ensemble complet des enregistrements dans lesquels il apparaît sous une forme cryptographiquement vérifiable, et migrer vers n’importe quel locataire fonctionnant selon le même modèle architectural. Une interface de dialogue supervisée — file d’attente éditoriale validée par l’opérateur, porte de publication des brouillons, pas de publication automatique, pas de messagerie vers l’extérieur — étend l’interface utilisateur de gouvernance en lecture seule des parties prenantes à une gouvernance participative sans renoncer à la discipline de supervision.

L'architecture fonctionne en production sur une infrastructure relevant de la souveraineté de l'UE (OVH France) et de la Nouvelle-Zélande (Catalyst Cloud). Une configuration de partage de ressources est en cours de développement en tant que premier déploiement envisagé de fédération multi-instances. L'infrastructure de fédération bilatérale est livrée de bout en bout avec une matrice complète de tests négatifs couvrant les lectures limitées au périmètre, le blocage des écritures entre locataires, l'exhaustivité des journaux d'audit, la discipline de citation, le comportement de mise en cache/obsolescence, les états de données dans les cas limites, l'application des limites d'autorisation et la résolution des conflits d'espaces de noms ; les liens de fédération actifs entre locataires indépendants restent en attente de la première activation du covoiturage multi-instances. L'architecture est conçue pour s'acquitter des obligations de gouvernance Te Tiriti

L'architecture est conçue pour s'acquitter des obligations de gouvernance du Te Tiriti sur les systèmes d'IA utilisant ou produisant des données maories, conformément aux principes prescriptifs du cadre Kaupapa Māori AI du Dr Taiuru [25b] (consentement maori + souveraineté des données sur le matériel de formation + responsabilité sur l’ensemble de la chaîne). La question plus ouverte que pose le Dr Taiuru [25a] concernant la personnalité juridique des agents IA constitués à partir des connaissances maories relève du domaine empirique de l’article complémentaire (Article B — Couches linguistiques situées, synopsis de l’article empirique complémentaire, publié) et y est traitée, et non dans le présent article. Un cadre de développement (Tractatus, Apache 2.0) consigne les consultations architecturales qui ont abouti à cette conception ; le registre persistant fait partie de la surface d’évaluation. Le substrat est construit par une petite équipe en Nouvelle-Zélande, sans capital-risque. Il s’agit d’une réponse architecturale à la question de savoir comment une infrastructure communautaire peut refuser les conditions de souveraineté par défaut des plateformes américaines sans renoncer au travail que cette infrastructure accomplit pour les communautés qu’elle sert.

Mots-clés : souveraineté des données, isolation des locataires, provenance cryptographique, fédération bilatérale, droits des personnes concernées, portabilité souveraine, Te Tiriti o Waitangi, personnalité juridique de l'IA, kaitiakitanga, héritage des politiques, EUPL-1.2, principes CARE, RGPD article 15, partenariat renforcé pour la sécurité des frontières, CLOUD Act, identifiants décentralisés.

---

1. Introduction

La plateforme par défaut à l'échelle communautaire est une instance SaaS détenue par une société américaine, hébergée sur une infrastructure contrôlée par les États-Unis, monétisée par l' extraction d'attention, et régie par des conditions que l'opérateur peut modifier unilatéralement. L'omniprésence de cette norme par défaut n'est pas le résultat d'un accord fondé sur des valeurs communes conclu par des utilisateurs individuels ou des communautés après avoir pesé le pour et le contre des alternatives. Elle est le résultat de

plus d'une décennie d' investissements soutenus des entreprises pour façonner les attentes des utilisateurs, mettre en place des mécanismes de verrouillage par effet de réseau et créer un cadre dans lequel les arrangements alternatifs sont rendus impraticables ou invisibles. Ces conditions restent en vigueur en permanence, indépendamment du consentement de la communauté, et ne se manifestent que de manière intermittente sous forme d'échecs visibles — un compte bloqué, une publication supprimée, un service fermé sans préavis, une révision des conditions d'utilisation allant à l'encontre de l'intérêt de la communauté — tandis que l'accord sous-jacent reste en vigueur en permanence. Pour certaines communautés — les communautés maories soumises aux obligations du Te Tiriti, les organismes professionnels dont les membres détiennent des informations confidentielles, les groupes d'histoire familiale conservant des archives sur des personnes vivantes identifiées, les groupes de conservation dont les données de localisation sont sensibles, les réseaux paroissiaux, les fédérations sportives, les communautés de langues minoritaires et d'autres dont le mode de vie ne se réduit pas à un profil — les conditions sous-jacentes sont insupportables : elles constituent des obstacles structurels au travail pour lequel la communauté existe.

Cet article s'adresse à ces communautés — et à la catégorie plus large de petites organisations qu'elles incarnent : des organisations détenant des informations confidentielles sur des infrastructures hors de leur champ de compétence, selon des conditions que seul l'opérateur peut réviser.

Trois pressions s'exercent sur ces communautés.

La première est **d'ordre juridictionnel**. Le CLOUD Act (2018) [9] étend l'autorité des États-Unis en matière de mandats aux fournisseurs de services cloud détenus par des entités américaines partout dans le monde, quel que soit le lieu de résidence de la personne concernée. Les négociations relatives au Partenariat renforcé pour la sécurité aux frontières (EBSP), actuellement en débat public dans le contexte néo-zélandais [13][14], sont liées à la poursuite de la participation au programme américain d'exemption de visa, avec une date limite fixée pour les pays en négociation [13][14][15], et envisagent un accès élargi aux données, y compris aux informations biométriques et autres données d'identité [16][17]. Un commentaire juridique de l' université d'Auckland [18] observe que la documentation du département américain de la sécurité intérieure décrit les dispositions de l'EBSP comme allant bien au-delà des transferts au cas par cas prévus par les accords existants sur les données des dossiers passagers (PNR), laissant entrevoir la possibilité d'un accès direct aux bases de données. La Privacy Foundation New Zealand a fait part de ses préoccupations concernant la transparence et les garanties [19]. Dans ce contexte, la souveraineté n'est pas un terme marketing : il s'agit de savoir quel État peut exiger la divulgation, selon quel calendrier et avec quel préavis à la communauté dont les données sont divulguées.

Le deuxième aspect est **réglementaire**. Le Te Tiriti o Waitangi (le Traité de 1840 entre la Couronne et les Maoris), la loi européenne sur l'IA [6], les articles 9 et 15 du RGPD [8] et la loi européenne sur la liberté des médias [7] imposent chacun des obligations aux infrastructures de données communautaires qu'il est difficile voire impossible de respecter par délégation. Un opérateur de plateforme qui ne peut pas démontrer quel modèle a évalué le contenu de quel membre, au regard de quelles politiques rédigées par la communauté, et avec quelle décision, ne peut pas répondre aux obligations énoncées par ces instruments. Une plateforme qui ne peut pas fournir à un membre, sur demande, l'ensemble complet des enregistrements que ce membre a créés sous une forme vérifiable, ne peut pas satisfaire au droit d'accès prévu à l'article 15 du RGPD. Les communautés opérant sous le Te Tiriti sont soumises à une obligation correspondante en vertu de l'article 2 — rangatiratanga sur les taonga — qu'une architecture doit soutenir structurellement plutôt que de se contenter de la déclarer.

Le troisième aspect est **technique**. La pile d'IA standard achemine l'inférence via un petit nombre de fournisseurs d'infrastructure américains et traite le contenu de chaque communauté comme une donnée d'apprentissage potentielle. Pour les communautés dont le

vocabulaire, les protocoles de gouvernance ou les documents sacrés ne peuvent être intégrés sans préjudice dans un corpus mondial — et dont les obligations au titre du Te Tiriti ou des principes CARE seraient violées par une telle intégration —, la pile standard est inapplicable.

Cet article présente une réponse architecturale. L'engagement central est concret : chaque enregistrement de contenu porte sa propre provenance, sa propre politique d'accès et une chaîne cryptographique de chaque frontière de gouvernance qu'il a franchie. Les lectures exposent cet état aux consommateurs ; les écritures y ajoutent des éléments ; les suppressions le marquent comme obsolète. L'architecture fonctionne en production à travers de multiples configurations de type « village » sur des infrastructures relevant de la souveraineté de l'UE et de la Nouvelle-Zélande. Le travail a été entrepris sans capital-risque, avec le budget d'une petite équipe, par une entreprise privée néo-zélandaise, en utilisant un cadre de gouvernance en temps de développement (Tractatus) qui enregistre ses propres décisions architecturales au fur et à mesure.

L'article est organisé comme suit. La section 2 présente le contexte — le cadre de gouvernance en phase de développement, le Te Tiriti et les principes CARE qui encadrent la souveraineté des données autochtones (avec l'argumentation à deux registres de Taiuru (2026) sur les obligations du Te Tiriti et la question ouverte de la personnalité juridique des agents IA abordée au §3.6), la définition opérationnelle des *enregistrements souverains*, le cadre bilatéral de la fédération, et le cadre « membre en tant que sujet de données » pour la portabilité souveraine. Le §3 positionne ce travail par rapport à la littérature connexe, y compris l'engagement avec l'argument du Dr Taiuru en tant qu'ouvrage publié cité. La section 4 formalise le modèle de menace avec des adversaires nommés et des prédicats vérifiables. La section 5 énonce les principes de conception. La section 6 rend compte de la mise en œuvre architecturale. La section 7 rend compte de la fédération en production. La section 8 rend compte de la portabilité souveraine. La section 9 rend compte de l'interface utilisateur de gouvernance des parties prenantes, y compris l'interface de dialogue participatif supervisé de la phase 6 livrée. §10 présente un exemple concret de transfert de souveraineté de nommage interdomaines entre deux modules linguistiques situés. §11 passe en revue les configurations de type « village ». §12 rend compte de l'évaluation. §13 décrit la stratégie open source. §14 énonce la contribution architecturale. §15 énumère ce que l'architecture ne fait pas encore.

---

2. Contexte

2.1 Le cadre Tractatus

Le mécanisme de gouvernance en phase de développement utilisé pour construire et exploiter la plateforme est le cadre Tractatus, un projet de recherche distinct mené par le même auteur. Ce cadre comprend un ensemble de modèles architecturaux et de services de code pour la gouvernance de l'IA pendant le développement — principalement, des services qui interviennent dans la prise de décision d'un assistant de codage IA aux points de choix architecturaux. Le framework est open source sous licence Apache 2.0 et distribué publiquement sur `codeberg.org/mysovereignty/tractatus-framework` [1]. Un document de travail rend compte des observations issues du framework et des modèles architecturaux qu'il codifie ; les chiffres quantitatifs spécifiques sont présentés dans ce document de travail plutôt que de être repris ici.

Tractatus est une gouvernance *en phase de développement*: il façonne le code source et les choix architecturaux de la plateforme, et non ses requêtes d'exécution. La plateforme consulte le cadre aux points de décision architecturale et conserve chaque consultation sous forme d'enregistrement dans la base de données de la plateforme ; les consultations sont stockées par identifiant de révision, service, liste de conditions et verdict RÉUSSI/ÉCHOUÉ.

La discipline consistant à enregistrer la consultation — de manière uniforme dans les bases de données de production locales ainsi que celles relevant de la souveraineté de l'UE et de la Nouvelle-Zélande, automatisée par des scripts par décision — constitue la contribution ; un futur lecteur pourra demander quelles conditions une décision architecturale particulière a traitées, et la réponse se trouve dans la base de données, et non dans le texte.

Cette distinction est importante. Tractatus est le cadre. La plateforme en est une application. Cet article rend compte de la plateforme ; le cadre est mentionné par souci d'exhaustivité, car le code source de la plateforme le consulte à chaque point de décision architecturale.

2.2 Te Tiriti o Waitangi et la souveraineté des données autochtones

Le Te Tiriti o Waitangi, traité de 1840 conclu entre la Couronne britannique et les iwi maoris, constitue le fondement du droit constitutionnel néo-zélandais. Ses trois articles — reconnaissant la souveraineté tribale sur les taonga (objets précieux), l'autorité de gouvernance de la Couronne et l'égalité de citoyenneté — définissent les obligations actuelles en matière de données. Le rapport *WAI 262* du Tribunal de Waitangi [5] et les *principes CARE pour la gouvernance des données autochtones [* 4] sont des formulations largement citées de ce que ces obligations impliquent pour l'infrastructure des données communautaires. Les principes CARE — Bénéfice collectif, Autorité de contrôle, Responsabilité, Éthique — ne sont pas identiques aux principes FAIR pour les données ouvertes ; ils coexistent avec ces derniers et prévalent explicitement en cas de conflit entre les deux.

Un rapport plus récent du Tribunal, *WAI 2522* [13a], a étendu l' analyse aux instruments économiques internationaux — l'enquête sur le Partenariat transpacifique, l'accord de médiation et la mise en œuvre de ces instruments par le ministère des Affaires étrangères et du Commerce. Les conclusions du Tribunal dans le rapport WAI 2522, parallèlement au travail de Ngā Toki Whakarururanga en tant que vecteur d'engagement entre les Māori et la Couronne, renforcent cette obligation : une Couronne qui expose les données des Māori à un régime juridictionnel étranger — par le biais d'interdictions de localisation des données dans les traités commerciaux, par l'exposition au CLOUD Act, ou par le biais d'un partenariat renforcé pour la sécurité aux frontières qui envisage un accès direct aux bases de données — ne peut satisfaire à la protection des taonga prévue par l'article 2 à moins que l'architecture elle-même n'empêche une telle exposition. La souveraineté architecturale est la seule souveraineté qui résiste à l'examen de l'article 2 une fois que les obligations conventionnelles de la Couronne créent des voies d'exportation.

Pour les communautés maories faisant valoir leurs droits en vertu du Te Tiriti, une plateforme communautaire doit leur permettre de conserver leurs données sur une infrastructure qu'elles peuvent auditer, régie selon leurs tikanga (protocoles coutumiers), sans aucune possibilité d'accès intercommunautaire — y compris par l' opérateur de la plateforme. L'architecture répond directement à cela : l'isolation des locataires est le principe fondamental, et non une fonctionnalité. Un opérateur de plateforme disposant d'un accès au niveau du contenu aux données des locataires ne peut pas satisfaire à l' obligation des principes CARE relative *au pouvoir de contrôle*.

Le Dr Karaitiana Taiuru (Ngāi Tahu, Ngāti Kahungunu) a publié de nombreux travaux sur l'éthique technologique maorie, la souveraineté des données autochtones, l'éthique de l'IA et les droits numériques ; ses travaux sont disponibles sur taiuru.co.nz. La couche linguistique contextuelle « Village » qui fonctionne sur la plateforme présentée ici a été entraînée sur les cadres publiés par le Dr Taiuru avec son autorisation, et avec mention de la source. L'ensemble des travaux du Dr Taiuru sur la gouvernance de l'IA maorie constitue le point de référence permanent de la position adoptée dans cet article. Son cadre Kaupapa Māori AI [25b] (mars 2026), exprimé dans le whakatauāki *He Tangata, He Karetao, He Ātārangi* (une personne, une marionnette, une ombre), mentionne le consentement maori et la souveraineté des données sur les connaissances utilisées dans l'entraînement de l'IA, ainsi

que la responsabilité tout au long de la chaîne entre développeurs, opérateurs et déployeurs, en tant que pratiques obligatoires fondées sur le Te Tiriti et la sur les droits des peuples autochtones. Les primitives architecturales présentées dans cet article sont conçues pour mettre en œuvre ces pratiques obligatoires. Une étude plus récente du Dr Taiuru [25a] pose, séparément, la question ouverte de savoir si et dans quelles conditions la personnalité juridique pourrait être étendue aux agents d'IA constitués à partir des connaissances maories — en s'appuyant sur la conclusion de la WAI 2522 selon laquelle les données maories sont des taonga et sur le précédent des trois lois sur la personnalité juridique des entités naturelles (Te Urewera 2014 ; Te Awa Tupua 2017 ; Te Kāhui Tupua 2025) — une question qu'il renvoie expressément au travail collectif entre les développeurs d'IA, les agences gouvernementales et les communautés maories . L'enquête sur la personnalité juridique relève du domaine empirique du document d'accompagnement B (résumé du document d'accompagnement empirique, publié), où sont décrits le modèle architectural de la couche linguistique située et les principes de fonctionnement, et où le document empirique complet rendra compte en détail de la discipline de formation des cohortes sur laquelle s'appuierait tout futur engagement de partenariat par cohorte (y compris avec le test Tikanga de Mead) ; le présent document ne préjuge pas de ces travaux.

L'architecture ne vise pas spécifiquement les communautés maories. La même propriété — une plateforme qui ne peut pas voir au-delà des communautés — répond aux obligations réglementaires auxquelles sont confrontées les communautés de langues minoritaires de l'UE en vertu de la loi européenne sur la liberté des médias et des protections des catégories spéciales prévues à l'article 9 du RGPD, où les données culturelles des langues minoritaires sont raisonnablement considérées comme une catégorie spéciale. Une communauté galloise, une communauté sami, une communauté sorabe, une communauté frisonne, une communauté catalane peuvent adopter la même architecture en réentraînant la couche linguistique sur un corpus différent et en réécrivant la politique dans le cadre de leur propre cadre juridique ; l' architecture elle-même est portable. Cette portabilité est une propriété architecturale centrale.

2.3 Pourquoi « enregistrements souverains » plutôt que « chiffrés au repos »

L'expression « *enregistrement souverain* » est intentionnelle. Le chiffrement au repos est une fonctionnalité ; la souveraineté est une propriété architecturale. Un enregistrement est souverain au sens où nous l'entendons ici lorsque chacune des conditions suivantes est vérifiée :

1. Il porte sa propre provenance — qui l'a rédigé, qui en est le kaitiaki (gardien), selon quel tikanga il a été partagé, quand il a été créé, et un hachage cryptographique reliant ces champs entre eux.
2. Il est assorti de sa propre politique : qui peut le lire, qui peut s'entraîner dessus, qui peut l'exporter, que se passe-t-il en cas de conflit de politiques.
3. Il comporte sa propre chaîne de preuves — chaque étape de gouvernance qu'il a franchie (création, mise à jour, exportation, suppression) est enregistrée avec une signature cryptographique.
4. Le cache de son état de vérification est observable au moment de la lecture — chaque utilisateur de l'API voit si la chaîne de l'enregistrement est à jour, expirée, incohérente ou invérifiable, sans avoir à se fier à la parole de la plateforme à ce sujet.
5. Il est transférable à la demande d'un membre. Un membre peut exporter l'ensemble complet des enregistrements dont il est l'auteur, le kaitiaki ou autrement désigné comme sujet des données ; l'exportation transmet la chaîne de preuve ; un vérificateur externe détenant le document d'identification publié du locataire source peut reconstituer chaque entrée signée contenue dans les enregistrements.

Il s'agit de propriétés opérationnelles, vérifiables à partir de l'interface API, et non de

propriétés théoriques. La suite de ce document décrit comment chacune d'entre elles est construite.

2.4 Fédération : bilatérale et délimitée

Une fédération, au sens où l'entend la plateforme, est un arrangement technique restreint qui permet à deux instances de locataires souveraines de se connecter à des fins spécifiques et délimitées — événements conjoints, covoiturage partagé, annonces inter-instances — sans que l'une ou l'autre ne cède ses données, son identité ou son autorité de gouvernance. Une fédération est un accord bilatéral : les constitutions des deux locataires s'accordent, les deux opérateurs s'accordent, le manifeste de la fédération est signé par les deux. Il n'y a pas de serveur central de fédération ; le flux de données est direct, la gouvernance est locale, et chacune des parties peut révoquer la fédération à tout moment.

Cela diffère structurellement du modèle de plateforme, où les instances sont les feuilles de l'arbre d'un seul opérateur. Cela diffère également structurellement du modèle dominant du fediverse, où la fédération est une propriété à l'échelle du réseau, gérée par un protocole partagé entre des serveurs contrôlés par des opérateurs. L'architecture décrite ici est bilatérale et délimitée : deux communautés s'accordent, selon des termes qu'elles spécifient, sur une interaction spécifique, et uniquement celle-ci.

La section §3 replace cela dans le contexte de la littérature connexe. La section §7 présente l' infrastructure de fédération qui a été déployée et l'état d'avancement de son déploiement en production. La section §10 propose un exemple concret de fédération bilatérale entre un module de connaissances botaniques et un module de revitalisation linguistique — une catégorie de fédération envisagée pour l'intégration dans les programmes scolaires en milieu primaire.

2.5 Le membre en tant que personne concernée

Un membre d'un tenant de registres souverains est, simultanément, un membre de la communauté (avec les droits sociaux, de gouvernance et de création de contenu que l'adhésion implique) et une personne concernée au sens des cadres réglementaires qui lui sont applicables. Un membre de la communauté de langue galloise est une personne concernée au sens du RGPD ; les données d'un membre de la communauté maorie relèvent à la fois des droits Te Tiriti de l'iwi et des droits individuels au titre du RGPD lorsque l'iwi exploite une infrastructure hébergée dans l'UE pour les membres de la diaspora ; un membre d'un Verein allemand est tout simplement une personne concernée au sens du RGPD.

L'architecture considère le cadre « membre en tant que personne concernée » comme prioritaire. Le bloc `metadata.origin` de chaque enregistrement désigne l' auteur et (le cas échéant) le kaitiaki, tous deux en tant qu'identifiants décentralisés. Le bloc `metadata.policy` de chaque enregistrement indique si et comment cet enregistrement peut être partagé, utilisé pour l'apprentissage ou exporté, et les conflits de politique sont résolus par la valeur par défaut constitutionnelle. L'exportation à l'initiative du membre (§8) prend la politique au pied de la lettre : la politique d'un enregistrement peut interdire son exportation même par son auteur (par exemple, une délibération fournie sous des conditions de consentement collectif), et le wrapper d'exportation applique cette règle. La souveraineté n'oppose pas les membres à la collectivité ; il s'agit du cadre architectural au sein duquel ces deux droits coexistent, et ce cadre rend le conflit explicite plutôt que de le dissimuler dans des choix de mise en œuvre.

---

3. Travaux connexes

L'architecture se situe à l'intersection de plusieurs axes de recherche et de développement actifs. Ce positionnement est crucial car la contribution ne consiste pas en l'introduction d'une primitive unique — des éléments de base bien connus sont réutilisés — mais en l'intégration de ces primitives dans un substrat qui répond au modèle de menace de la section 4 à partir du niveau de l'enregistrement vers le haut plutôt qu'à partir du niveau de l'opérateur vers le bas.

La revue de la littérature qui suit aux §§3.1–3.7 replace les engagements de cet article dans leur contexte de recherche. Les lecteurs intéressés par les arguments de gouvernance peuvent passer directement aux §7 (fédération en production), §8 (portabilité souveraine) ou §9 (interface utilisateur de gouvernance des parties prenantes), en retenant que les primitives de l'architecture — fédération bilatérale, portabilité souveraine, mécanismes de suppression cryptographique résistant à la compromission de l'opérateur — sont conçues pour résister au contournement en exécution dans le cadre du modèle de menace présenté au §4. La littérature ci-dessous établit comment chaque élément fondamental s'inscrit par rapport à son plus proche voisin dans la recherche publiée.

3.1 Infrastructure sociale fédérée

ActivityPub [Snell & Prodromou, 2018, Recommandation du W3C [20]] et l'écosystème Mastodon établissent la fédération comme une propriété à l'échelle du réseau médiée par un protocole partagé entre des serveurs contrôlés par des opérateurs . Dans la fédération ActivityPub, deux serveurs se fédèrent en échangeant des objets d’activité signés ; la granularité est par acteur et par activité, médiée par les points de terminaison de collecte du protocole. Cela est structurellement distinct de la fédération bilatérale et délimitée décrite ici. La contribution d’ActivityPub réside dans l’interopérabilité entre des milliers d’ instances ; la contribution de cet article réside dans la préservation de la souveraineté entre exactement deux instances à la fois, par le biais d’un manifeste signé, avec la révocation comme opération de premier ordre. Les deux architectures constituent des réponses valables à des postures de souveraineté différentes : ActivityPub optimise la portée du graphe ; cet article optimise l’autorité tribale/collective sur l’enveloppe de la fédération .

La littérature sur les médias sociaux décentralisés documente les propriétés des graphes de fédération, les compromis en matière de modération au niveau des instances et les lacunes en matière de portabilité du contenu. Les caractérisations empiriques du graphe Mastodon et des modèles de modération des instances [31][32] éclairent l’analyse opérationnelle des plateformes du fediverse ; des travaux ultérieurs sur le protocole AT [Bluesky Public Benefit Corporation, 2024 [21]] ont proposé la portabilité des comptes — les données d’un membre suivent le membre plutôt que le serveur — comme réponse structurelle au problème de la modération et de la découvrabilité. La portabilité souveraine abordée dans cet article (§8) est techniquement liée mais motivée différemment : la portabilité est un droit de la personne concernée en vertu de l’article 15 du RGPD, et le contrôle de conformité constitutionnelle du locataire destinataire (§8) est intégral, et non facultatif. La portabilité du protocole AT est axée sur le compte ; la portabilité décrite dans cet article est axée sur les enregistrements et respecte les politiques, avec un manifeste de liste de retenue couvrant les enregistrements dont la politique interdit l’exportation, même par leur auteur.

3.2 Identifiants décentralisés et informations d'identification vérifiables

La spécification W3C Decentralized Identifiers (DID) v1.0 [11] établit un schéma d'identificateurs indépendant de la méthode qui prend en charge plusieurs mécanismes de résolution. Les locataires et les membres de la plateforme publient des documents DID à des points de terminaison bien connus sous le domaine propre au locataire ; la vérification des opérations

cryptographiques (hachages de provenance, signatures de la chaîne de preuves, manifestes de fédération, paquets d'exportation) est effectuée par rapport à ces documents. Ce modèle suit la convention utilisée dans les travaux connexes cités aux sections 3.1 à 3.7 ; le choix architectural consiste à rendre chaque opération cryptographique du système vérifiable de manière indépendante en utilisant uniquement le document DID publié par le locataire source et des primitives cryptographiques standard — sans vérificateur tiers, sans racine de confiance partagée, sans registre centralisé.

3.3 Stockages de données Solid et personnels [Mansour et al., 2016 [22] ; W3C Solid Community Group] et la

Solid [Mansour et al., 2016 [22] ; W3C Solid Community Group] et la plateforme Inrupt placent les données dans des pods personnels appartenant à la personne concernée, les applications demandant l'accès via une autorisation basée sur WebID. L'architecture de Solid repose sur le principe *de données par individu*; celle du présent document repose sur *le principe de données par communauté, les membres étant considérés comme des personnes concernées de premier plan au sein de la communauté*. Les deux approches sont complémentaires plutôt que concurrentes : un pod Solid pourrait en principe servir de destination d'exportation pour un ensemble de records souverains, et une communauté dont les membres gèrent chacun des pods Solid pourrait en principe implémenter le tenant de records souverains de la plateforme par-dessus. Le choix de la plateforme de centrer l’ unité*communautaire* reflète une position de fond selon laquelle les communautés de langue minoritaire et autochtones ne sont pas des agrégats de sujets de données individuels : le collectif est le détenteur des droits sur les taonga (principe CARE : bénéfice collectif), et l’architecture doit servir l’autorité du collectif (autorité de contrôle).

3.4 Apprentissage fédéré et fiducies de données

L'apprentissage fédéré [McMahan et al., 2017 [23] ; Kairouz et al., 2021 [24]] se *distingue* de ce travail *sur le plan architectural*. L'apprentissage fédéré entraîne un modèle partagé en échangeant des mises à jour de gradients entre les parties détentrices de données sans échanger de données brutes. La fédération décrite dans cet article n'échange aucun paramètre de modèle — la fédération est un accord de données entre locataires sous manifeste signé, avec un flux de données défini par accord, et aucun modèle partagé n'est sous-entendu. La couche de langage situé de la plateforme est, par construction, propre à chaque locataire ; le partage des paramètres de modèle entre locataires violerait le principe fondamental d'isolation des locataires (§5.1). Les preuves empiriques issues de la discipline de l'apprentissage concernant la couche de langage situé sont présentées séparément dans l'article B (résumé de l'article empirique d'accompagnement, publié).

Les trusts de données — tels que développés dans la définition de travail de l’Open Data Institute d’un trust de données comme « une structure juridique qui assure une gestion indépendante des données » [33] et dans les recherches parallèles d’Element AI sur la conception institutionnelle des trusts de données en tant que mécanisme visant à remédier aux asymétries de pouvoir entre les entreprises technologiques, le gouvernement et le public [34] — introduisent un tiers de confiance qui détient les données au nom d’une communauté et en gère l’accès. L’architecture présentée dans cet article ne comporte pas un tel tiers de confiance. L’ opérateur de la plateforme peut gérer les opérations d’infrastructure (créer des locataires, gérer la facturation, surveiller l’état de santé) mais ne peut pas lire le contenu des locataires. Il n’existe aucun rôle dans le système qui agrège les données entre locataires, même temporairement. La force d’une fiducie de données réside dans l’intermédiation institutionnelle ; la force de cette architecture réside dans l’impossibilité d’une intermédiation depuis l’intérieur de la plateforme.

3.5 Mise en œuvre des articles 15 et 20 du RGPD Le

Le droit d'accès (article 15) et le droit à la portabilité des données (article 20) du règlement général sur la protection des données [8] font l'objet d'une abondante littérature sur leur mise en œuvre — notamment Wachter, Mittelstadt & Floridi [26] sur le débat relatif aux droits à l'explication, et Edwards & Veale [27] qui soutiennent que le droit à l'effacement (article 17) et la portabilité des données (article 20) ont plus de poids pratique que les droits à l'explication pour la responsabilité algorithmique. Le point de terminaison DSR de la plateforme (§8) met en œuvre les six droits pertinents (articles 15, 16, 17, 18, 20, 21) via un pipeline d'exportation uniforme des enregistrements souverains qui renvoie les enregistrements de la personne concernée avec une préservation complète de la chaîne de preuves, aux formats JSON, CSV ou PDF, sous la forme d'un ensemble canonique unique. La nouveauté technique réside ici dans la *vérifiabilité cryptographique* de cet ensemble : toute partie externe disposant du document DID publié par le locataire source peut vérifier chaque entrée contenue dans les enregistrements de l'ensemble, sans avoir à faire confiance ni au locataire source ni à la partie destinataire choisie par la personne concernée. Les implémentations standard de l'article 15 renvoient des données ; cette implémentation renvoie des données*vérifiables*.

3.6 Principes CARE et gouvernance autochtone des données

Les principes CARE [4] définissent une obligation de fond qui a des implications architecturales : *le pouvoir de contrôle* exige que la communauté — et non l'opérateur de la plateforme, ni un tiers fiduciaire, ni un régulateur disposant d'un pouvoir d'assignation en dehors de la juridiction de la communauté — puisse gouverner les données selon ses propres conditions. Travaux ultérieurs sur la gouvernance des données autochtones — Walter & Suina [25] sur les données autochtones et les méthodologies ; *les Principes de souveraineté des données maories* de Te Mana Raraunga [28] ; Carroll, Rodriguez-Lonebear & Martinez [29] sur les stratégies des nations autochtones américaines ; Hudson, Anderson, Dewes, Temara, Whaanga & Roa [30] sur la conceptualisation du big data à travers le prisme maori — ont détaillé les implications tout au long du cycle de vie des données (collecte, stockage, traitement, partage, archivage). Le choix architectural de la plateforme — l'isolation des locataires comme fondement, les enregistrements souverains comme substrat, la fédération bilatérale comme seul mécanisme inter-locataires — est une réponse technique aux obligations CARE ; ce n'est pas la seule réponse possible, mais c'est une réponse architecturale qui résiste à l'examen de l'article 2 du Tiriti dans le cas spécifique des données des iwi néo-zélandais et de la pression juridictionnelle de type EBSP.

Les travaux du Dr Taiuru sur la gouvernance de l'IA maorie [25a, 25b] (présentés au §2.2) traduisent les obligations CARE en engagements architecturaux spécifiques. L'obligation normative — consentement maori et souveraineté des données sur les connaissances utilisées dans l'entraînement de l'IA, responsabilité tout au long de la chaîne pour les développeurs et les opérateurs, et obligations du Te Tiriti concernant les systèmes d'IA utilisant ou produisant des données maories — s'applique désormais à toute plateforme dont les interfaces d'IA touchent à des éléments taonga. Les primitives architecturales décrites dans cet article (l'isolation des locataires en tant que rangatiratanga au titre de l'article II sur les données ; l'entraînement par cohorte par locataire en tant que lieu du comportement du modèle déterminé par la communauté pour les locataires maoris ; l'interface de dialogue supervisée de la phase 6 (§9) en tant que supervision kaitiaki sur ce que l'interface émet ; la finalité de la suppression cryptographique en tant que rangatiratanga sur ce qui est oublié ; l'attribution basée sur le DID et la chaîne de preuve en tant que traçabilité whakapapa de chaque enregistrement) sont conçues comme une réponse structurelle à cette obligation normative. La question supplémentaire posée par le Dr Taiuru [25a] — à savoir si et dans quelles conditions la personnalité juridique pourrait être étendue aux agents IA constitués par le savoir maori, sur le précédent de Te Urewera (2014), Te Awa Tupua (2017) et Te Kāhui Tupua (2025) — est traitée dans le document d'accompagnement B au niveau de la discipline

de formation des cohortes, et n'est pas abordée dans le présent document.

3.7 Menaces connexes : l’exploitation minière dans le cloud étranger via l’IA de pointe

Les commentaires de l’industrie sur l’architecture de l’IA souveraine [22b][23b][24b] ont analysé la convergence des cadres d’accès légal américains (CLOUD Act ; FISA) et du déploiement de modèles d’IA de pointe sur une infrastructure cloud contrôlée par les États-Unis comme une voie de risque combinée : les données consultées sous contrainte légale étrangère peuvent être exploitées à grande échelle par des modèles d’IA de pointe à la recherche de schémas dépassant le champ de divulgation initial. Les implications pour les données biométriques, d’identité et d’authentification sont particulièrement graves. La réponse architecturale proposée par cet article est que les identifiants critiques et les données biométriques ne doivent jamais se trouver dans une infrastructure cloud accessible depuis l’étranger, et que toute interaction d’un LLM avec des données souveraines passe par une interface gérée par le locataire, où ce dernier limite ce qu’un modèle externe peut apprendre ou conserver.

---

4. Modèle de menaces

Cette section formalise les menaces auxquelles l'architecture est conçue pour résister. Le modèle identifie six adversaires, énonce les invariants de souveraineté que chacun ne doit pas violer, et résout chaque invariant en un prédicat vérifiable.

4.1 Adversaires

A1. Opérateur d'hébergement contraint par une juridiction. Un opérateur de plateforme qui est lui-même contraint par un régime juridique étranger — une ordonnance au titre du CLOUD Act, un mandat FISA, une disposition relative à l'accès à la base de données du Partenariat pour la sécurité renforcée des frontières , une disposition équivalente en vertu d' une autre juridiction — de divulguer les données des locataires auxquelles il a techniquement accès. Cette contrainte peut s'accompagner d'une ordonnance de non-divulgation. L'opérateur peut agir de bonne foi, de mauvaise foi ou sous la contrainte ; l' architecture est indifférente au motif de l'opérateur et envisage le pire scénario. La catégorie des adversaires n’est pas hypothétique : voir, par exemple, la fuite de données Instructure / Canvas de mai 2026, au cours de laquelle environ 275 millions d’enregistrements provenant de 8 809 établissements d’enseignement ont été exfiltrés d’un seul opérateur de technologies éducatives (couverture médiatique multiple, notamment par Malwarebytes, TechCrunch et SecurityWeek ; la violation a été revendiquée par le groupe ShinyHunters ; Instructure a confirmé l’accès non autorisé).

A2. Co-locataire. Un autre locataire sur la même infrastructure de plateforme qui tente de lire du contenu qui ne lui appartient pas, que ce soit par la construction de requêtes, la connaissance du schéma, l'escalade de privilèges ou l'exploitation d'une ressource partagée (base de données, cache, système de fichiers).

A3. Homologue de fédération inter-locataires. Le locataire situé de l’ autre côté d’un accord de fédération bilatéral, qui tente d’accéder à des données en dehors de l’objectif défini dans le manifeste, ou dont la propre infrastructure est elle-même compromise sur le plan juridictionnel (attaque de la chaîne de confiance via la fédération).

A4. Membre-attaquant. Un membre d’un locataire qui tente d’accéder à du contenu qu’il n’est pas autorisé à lire (par exemple, les délibérations privées d’un autre membre, un enregistrement réservé à un sous-groupe dont il n’est pas membre), ou qui tente d’exercer

une autorité qu'il ne détient pas (par exemple, effectuer une opération d'administration du locataire, modifier la constitution).

A5. Exploitation de données dans un cloud étranger via une IA de frontière. Un adversaire qui a obtenu de force l'accès aux données via A1, puis achemine les données à travers un modèle d'IA de frontière pour extraire des schémas qui dépassent le cadre légal de la divulgation initiale — corrélation biométrique entre les populations, inférence de schémas d'authentification à partir des métadonnées de session, reconstruction de graphes sociaux à partir des traces d'interaction.

A6. Adversaire exploitant les données biométriques. Un adversaire qui, en combinant A1 (hôte contraint juridiquement) et A5 (exploitation de données dans le cloud étranger via une IA de frontière), cherche à exploiter les données biométriques conservées par la plateforme — visages, empreintes digitales, empreintes vocales, scans de l'iris, profils biométriques comportementaux — pour identifier, corréler ou contraindre les membres. L'influence de l'adversaire s'accroît avec le caractère irrévocable des données biométriques : un mot de passe divulgué peut être modifié, une empreinte faciale divulguée ne le peut pas. La portée de l'adversaire est amplifiée par les trois voies convergentes d'exposition des données biométriques relevant de la juridiction américaine — capture directe du côté américain aux frontières et lors des entretiens de visa, hébergement sur le cloud américain sous la contrainte du CLOUD Act, et futurs accords de partenariat renforcé pour la sécurité aux frontières envisageant un accès direct aux bases de données biométriques des pays partenaires. La réponse architecturale est que la plateforme ne conserve aucune donnée biométrique d'aucune sorte sur aucune des voies qu'elle contrôle (voir §5 principes de conception et §13.1 discipline des fournisseurs).

A7. Attribution erronée via un agent d'agrégation. Une future interface d'agent — en exécution, persistante, orientée vers un objectif — qui agrège du contenu entre locataires ou entre enregistrements au sein d'un locataire de manière à échapper à la politique `de partage` au niveau de l'enregistrement ou à l'attribution kaitiaki au niveau de l'enregistrement ; ou qui produit des attributions émergentes (paternité, kaitiakitanga, relations portrices de tikanga) que les enregistrements sous-jacents ne justifient pas. Le runtime de la plateforme comprend aujourd'hui une distribution en un seul tour au niveau de la couche de langage située (§5 principes de conception) et l'interface de dialogue participatif mdsl de la phase 6 (§9), qui est elle-même supervisée en un seul tour — file d'attente éditoriale validée par l'opérateur, porte de publication des brouillons, pas de publication automatique, pas de messagerie vers l'extérieur. Aucune de ces deux interfaces ne présente le mécanisme technique complet de A7 (autonomie + Aucun des deux ne présente le mécanisme technique complet de A7 (autonomie + persistance + agrégation inter-enregistrements). Le devoir de gouvernance du Te Tiriti que le Dr Taiuru (2026) affirme (voir §3.6) porte sur la charge substantielle de cet adversaire — à savoir que toute émission inter-enregistrements ou inter-locataires provenant d'un locataire porteur de Māori emporte ce devoir, quel que soit le niveau d'autonomie de l'interface. L'invariant I3 existant de l'architecture L'invariant I3 existant de l'architecture (divulgation respectueuse des politiques) constitue la principale défense technique : chaque émission inter-enregistrements ou inter-locataires est soumise à un contrôle de conformité aux politiques à la limite de la route ; l'attribution kaitiaki et la chaîne de preuve assurent la traçabilité whakapapa à travers chaque enregistrement ; la file d'attente éditoriale de phase 6 + le contrôle de publication des brouillons (calquée sur le précédent « publication sur instruction uniquement » de Mastodon) constitue la discipline contre l'émergence silencieuse de comportements plus forts par rapport à la base de référence supervisée. En adoptant le conseil plus large du Dr Taiuru — selon lequel la conformité au tikanga est bien plus facile à intégrer dès le départ qu'à mettre en place a posteriori — A7 est nommé ici afin que toute évolution future vers l'autonomie ou la persistance hérite de la propriété de refus en tant qu'invariant de conception plutôt que comme un correctif.

4.2 Invariants de souveraineté

Pour chaque adversaire, l'architecture défend un ou plusieurs invariants :

I1. Isolation du contenu du locataire. Aucun opérateur de plateforme, aucun colocataire, aucun processus automatisé en dehors du contexte de requête propre au locataire ne peut lire le contenu du locataire. (Protège contre A1, A2.)

I2. Authenticité de la provenance. L'auteur et le kaitiaki de chaque enregistrement de contenu sont cryptographiquement liés au contenu de l'enregistrement ; aucun de ces champs ne peut être modifié en silence sans invalider le cache de vérification. (Protège contre A1, A4.)

I3. Divulgation respectueuse des politiques. Tout flux de données inter-locataires ou transfrontalier respecte le paramètre `metadata.policy.share_within` de l'enregistrement et l'objectif délimité du manifeste de fédération ; les flux sortant de ce cadre sont refusés à la limite de la route. (Protège contre A1, A3.)

I4. Caractère définitif de la suppression cryptographique. Les enregistrements dont `metadata.policy.delete_must_be_cryptographic` est défini sont supprimables de manière à rendre le texte chiffré irrécupérable à partir de l' état persistant, même par l'opérateur de la plateforme disposant d'un accès complet à la base de données . (Protège contre A1, A5.)

I5. Intégrité du manifeste de fédération. Une fédération bilatérale ne s'active pas tant que les signatures des deux parties n'ont pas été vérifiées par rapport à leurs documents DID publiés respectifs ; la révocation est elle-même un événement signé ; aucun tiers ne peut contourner une fédération. (Protège contre A3.)

I6. Reconstructibilité de l'audit. Chaque événement transfrontalier (création, mise à jour, exportation, suppression, activation de la fédération, révocation de la fédération, changement d'adhésion) laisse une entrée signée dans la chaîne de preuves ; le locataire peut reconstituer chaque événement à partir de sa propre base de données sans avoir à se fier aux déclarations de l'opérateur de la plateforme. (Protège contre A1, A3.)

I7. Honnêteté en matière de portabilité souveraine. L'exportation des droits d'accès d'un membre est filtrée par le même contrôle de politique qui régit les lectures ordinaires ; les enregistrements dont la politique interdit l'exportation sont répertoriés dans le manifeste d'exportation comme étant retenus, avec mention de la raison invoquée par la politique. (Protège contre A4 et préserve la capacité de A1 à affirmer « nous avons exporté à la personne concernée tout ce qu'elle était en droit de recevoir »).

I8. Limitation de l'exploration hors plateforme. Aucun enregistrement de contenu ne quitte la base de données du locataire sous forme de texte en clair, sauf via un itinéraire qui a été vérifié au regard de la constitution du locataire ; l'inférence IA en temps réel (couche linguistique située) s'exécute sur une infrastructure contrôlée par le locataire avec des entrées filtrées par la politique. (Protège contre A5.)

I9. Pas de collecte de données biométriques. La plateforme ne collecte, ne stocke et ne traite aucune donnée biométrique d'aucune sorte sur aucun chemin qu'elle contrôle — pas d'empreintes faciales, pas d'empreintes digitales, pas d'empreintes vocales, pas de modèles d'iris, pas de profils biométriques comportementaux, pas de clés dérivées de données biométriques. (Protège contre A6 ; renforce A1 — l'opérateur ne peut être contraint de divulguer ce qui n'a jamais été collecté ; renforce A5 — il n'existe aucune surface d'exploration biométrique.)

4.3 Prédicats vérifiables

Chaque invariante se résout en un ou plusieurs prédicats testables à partir de l' interface API ou par inspection directe de la base de données.

Pour I1 (isolation du contenu des locataires) : toutes les requêtes portant sur des collections relevant d'un locataire sont construites de telle sorte que l'omission d'un filtre de locataire génère une erreur d'exécution ; une suite de tests automatisés vérifie ceci. Le plugin de contexte de requête `basé sur AsyncLocalStorage` de la plateforme applique ce prédicat ; les requêtes hors du contexte de requête (tâches planifiées, traitements par lots) doivent explicitement se désengager et en documenter la raison.

Pour I2 (authenticité de la provenance) : pour tout enregistrement `r`, `recompute_provenance_hash(r.meta == r.metadata.origin.provenance_hash`; la sérialisation en forme canonique est stable en mode d'hydratation (un incident du 22/04/2026 , au cours duquel 25 tests unitaires ont été réussis sans problème alors que les hachages des documents Real-Mongoose divergeaient par rapport au moment de l'enregistrement, a mis en évidence cette exigence). La validation des cas d'utilisation (§12) vérifie la stabilité des hachages entre les modes d'hydratation.

Pour I3 (divulgation respectueuse des politiques) : pour toute émission inter-routes ou inter-WebSockets, la porte effective-policy est invoquée ; un enregistrement dont la valeur `share_within` ne figure pas dans le vocabulaire reconnu échoue avec le statut CLOSED et la raison `share_within_unknown_scope`; c'est la ligne de conduite du projet *: être honnête sur ce qui ne peut être vérifié ; ne pas inventer de* position *d'autorisation*. Un test automatisé met en place des scénarios de pairs de fédération et vérifie le comportement de la porte pour chacun d'entre eux.

Pour I4 (finalité de la suppression cryptographique) : pour tout enregistrement marqué `delete_must_be_cryptographic`, la suppression détruit la clé de chiffrement propre à l'enregistrement dans le magasin de clés du locataire ; les tentatives de lecture ultérieures renvoient « `unverifiable` » plutôt que « `valid` »; le texte chiffré au repos n'est pas récupérable par regénération de clé.

Pour I5 (intégrité du manifeste de fédération) : un manifeste de fédération porte les signatures des deux parties ; `verify_signature(manifest, party_a.did_document) == true && verify_signature(manifest, party_b.did_document) == true`; la fédération ne s'active pas si l'une des deux vérifications échoue ; un test statique vérifie qu' aucun chemin d'exécution n'active la fédération sans ces vérifications.

Pour I6 (reconstituabilité de l'audit) : pour toute séquence d'événements liée à un locataire, la chaîne de preuves sur chaque enregistrement concerné peut être reconstituée en lisant les entrées signées ; aucun événement n'est silencieux ; le module d'écriture du journal d'audit de l'architecture est appelé à partir d'un point de contrôle unique qui ne peut être contourné par un contrôleur ignorant l'appel.

Pour I7 (honnêteté de la portabilité souveraine) : pour une demande d'exportation au titre de l'article 15, la réponse comprend (a) le paquet canonique, (b) la liste des exclusions nommant chaque enregistrement exclu et la raison de la politique, (c) un accusé de réception signé couvrant les deux. Un test d'intégration vérifie que les enregistrements exclus sont bien exclus *et* répertoriés.

Pour I8 (limite d'exploitation hors plateforme) : la couche d'inférence d'exécution est hébergée sur une infrastructure contrôlée par le locataire ou approuvée par la communauté (dans le cas de la plateforme, OVH France sous souveraineté de l'UE ou Catalyst Cloud sous souveraineté néo-zélandaise, ou un basculement eGPU domestique désigné). Aucune requête vers un point de terminaison d'inférence contrôlé par les États-Unis ne figure dans le chemin de requête de production . Une règle d'interdiction des fournisseurs, appliquée par révision du code, répertorie explicitement les fournisseurs autorisés et interdits.

Pour I9 (pas de collecte biométrique) : une recherche dans l'arborescence source de la plateforme ne renvoie aucune correspondance pour les noms de bibliothèques ou d'API de gestion biométrique ; une analyse d'exécution des bases de données de la plateforme ne renvoie aucun champ de type biométrique ; un test statique vérifie qu'aucune bibliothèque

de gestion biométrique n'est importée nulle part dans le code source de la plateforme. L'engagement architectural est codifié dans la règle d'interdiction des fournisseurs (§13.1) et vérifié par une revue de code à chaque modification. Le déverrouillage biométrique local sur l'appareil du membre d'un coffre-fort de credentials contrôlé par le membre — Apple Secure Enclave, Android StrongBox, coffres-forts à jeton matériel — est autorisé et architecturalement invisible pour la plateforme ; les données biométriques ne franchissent jamais les limites de la plateforme.

Le modèle de menace n’est pas exhaustif. Il s’agit du modèle que l’architecture est *connue* pour défendre, avec des prédicats nommés que l’opérateur et les auditeurs externes peuvent tester. Les menaces non énumérées ci-dessus (attaques par chiffrement niable, attaques par canal auxiliaire contre le magasin de clés, attaques de la chaîne d’approvisionnement contre le framework Tractatus) ne relèvent pas du champ d’application du présent document mais sont suivies dans le cadre de la discipline opérationnelle du projet.

---

5. Principes de conception

5.1 L'isolation des locataires comme principe fondamental, et non comme fonctionnalité

Le premier engagement de l’architecture est que l’isolation des locataires constitue la primitive fondamentale. Chaque requête de base de données est filtrée par `tenantId`. Le filtre est appliqué par un plugin de base de données qui s’exécute dans un contexte de requête `AsyncLocalStorage`; les requêtes en dehors du contexte de requête (tâches planifiées, traitements par lots) doivent explicitement se désengager et en documenter la raison. Il n’existe aucun rôle d’administrateur de plateforme disposant d’un accès au contenu inter-locataires ; un utilisateur administrateur de plateforme peut créer et gérer des locataires (opérations d’infrastructure) mais ne peut pas lire le contenu des locataires. Il ne s’agit pas d’une option de configuration — cela est imposé par le code, et toute tentative d’accès inter-locataires est traitée comme une faille de sécurité. La discipline est durable. Un seul enregistrement en mémoire interne, marqué « ne jamais tronquer », énonce le principe : « L’isolation des locataires EST le produit. Sans elle, il n’y a pas de souveraineté. » Il s’agit d’une règle d’ingénierie interne, appliquée par la révision du code.

Cette discipline est durable. Un seul enregistrement en mémoire interne, marqué « ne jamais tronquer », énonce le principe : *« L'isolation des locataires EST le produit. Sans elle, il n'y a pas de souveraineté. »* Il s'agit d'une règle d'ingénierie interne, appliquée par la révision du code et par des tests automatisés qui échouent si une requête est construite sans filtre de locataire.

5.2 Métadonnées des enregistrements souverains sous forme de schéma uniforme

Chaque modèle de contenu participant à la souveraineté comporte le même bloc de métadonnées, appliqué via un plugin de base de données :

```
metadata: {
  origin: {
    author_did, kaitiaki_did, collective_id,
    tikanga_under_which_shared, created_at,
    provenance_hash, provenance_algorithm
  },
  policy: {
    share_within, share_exclude_jurisdictions, share_include_jurisdictions,
    collective_consent_required, collective_consent_body,
```

```
    train_flag, conflict_resolution_directive,
    delete_must_be_cryptographic, delete_propagates,
    expiry, individual_overrides_respected
  },
  cryptage : { id_clé, algorithme },
  chaîne_de_preuve : [{ limite_franchie, politique_évaluée_par, décision,
                 réserves_ajoutées, horodatage, algorithme,
                 signature, signataire_a_fait }],
  cache_de_vérification : { vérifié_le, hachage_de_la_chaîne_à_la_vérification,
                       algorithmes_vérifiés, revérifier_après }
}
```

Le schéma est identique pour tous les modèles de contenu générés par les locataires — Story, Poll, Event, Media, Album, Comment, ChatMessage, Deliberation, Correspondence, NewsPost, Resource, CommunityResource, ResourceBooking — ainsi que pour un ensemble étendu de surfaces intégrées (couverture de sous-documents pour EventMenu, Edition et autres). Le chemin de création de chaque modèle dérive l'origine via un assistant partagé ; le hook de pré-enregistrement du plugin calcule le hachage de provenance et signe l'entrée de création ; le hook de post-enregistrement met en cache l'état de vérification ; les lectures enrichissent chaque enregistrement d'un champ de vérification qui indique aux utilisateurs l'actualité du cache. L'uniformité est le point essentiel : il n'y a pas d'implémentation de souveraineté sur mesure par modèle, et donc aucun risque de régression de souveraineté par modèle.

5.3 Provenance cryptographique avec agilité algorithmique

La provenance est calculée en SHA-256 sur une sérialisation JSON canonique des champs obligatoires et facultatifs de l'origine. L'algorithme est nommé dans `provenance_algorithm`, de sorte qu'une migration future vers une autre primitive cryptographique (par exemple, les candidats post-quantiques du NIST) ne nécessite pas de modification du schéma — seulement un nouveau point d'entrée sous la même forme canonique. Les opérations de signature sur les entrées de la chaîne de preuves comportent de même leur Les opérations de signature sur les entrées de la chaîne de preuves comportent de même leur champ`d'algorithme`; le wrapper de flexibilité cryptographique de la plateforme prend actuellement en charge Ed25519 et est structuré pour accepter des algorithmes supplémentaires sans modification du code d'appel.

Ce choix est délibéré. Les enregistrements à longue durée de vie survivent aux primitives cryptographiques qui les signent. Une architecture qui code en dur sa primitive ne peut honorer une revendication de souveraineté qui dure plus longtemps que la durée de vie de la primitive.

L'horizon estimé pour les ordinateurs quantiques pertinents sur le plan cryptographique (CRQC) est de 10 à 30 ans. Les normes de signature post-quantiques du NIST ont été finalisées en août 2024 (FIPS 204 ML-DSA, basée sur les treillis ; FIPS 205 SLH-DSA, basée sur le hachage), établissant la voie de migration conforme aux normes ; l'enveloppe d'agilité algorithmique ci-dessus permet la transition sans modification au niveau de chaque site d'appel. Deux autres propriétés limitent le coût de la falsification par enregistrement sous la menace d'un CRQC : un enregistrement falsifié doit rester cohérent auprès de N vérificateurs indépendants détenant chacun leurs propres enregistrements de référence (le coût de la vérification distribuée s'ajoute au coût de la rupture cryptographique) ; et les mécanismes de substrat spécifiés dans §7 (fédération bilatérale) et §8 (portabilité souveraine) ne dépendent pas de l'intégrité de la signature par enregistrement. La dégradation de la primitive cryptographique ne se répercute pas sur les autres mécanismes du substrat.

5.4 Héritage des politiques avec calcul de la politique effective à la limite de lecture

La politique n'est pas un champ unique ; c'est une hiérarchie. Chaque locataire dispose d'une constitution souveraine déclarant ses valeurs par défaut ; chaque sous-groupe peut les remplacer ; le bloc `metadata.policy` de chaque enregistrement peut apporter des précisions supplémentaires. Au moment de la lecture, une politique effective est calculée pour le membre demandeur par rapport à la pile de politiques de l'enregistrement. Le moteur d' effectue ce calcul ; la porte est appliquée à la limite de la route via des invocations par liste et par détail.

Le moteur est testé à plusieurs niveaux : tests unitaires par règle, validation des cas d’utilisation par rapport à des bases de données locales en production, et une discipline selon laquelle les tests prouvent que le câblage fonctionne dans les simulacres, mais les cas d’utilisation prouvent qu’il fonctionne dans la réalité. Ce dernier engagement — intériorisé après un incident au cours duquel une suite de tests unitaires substantielle a été validée sans faille pour une fonctionnalité qui était, en production, non câblée — est documenté dans la discipline opérationnelle du projet.

Trois options de filtrage restreignent l'accès à des modèles d'accès spécifiques : origin-only limite les lectures aux identifiants d'auteur de l'enregistrement ; group-scope limite les lectures aux membres du sous-groupe `collective_id` de l'enregistrement ; le mode strict unknown-scope échoue CLOSED pour toute valeur `share_within` que la porte ne reconnaît pas — défense en profondeur contre les configurations de locataires mal configurées ou les enregistrements importés par la fédération comportant des valeurs de portée en dehors de l’ ensemble reconnu par la plateforme.

5.5 Fédération bilatérale en production

La fédération, au sens du présent document, correspond à l’arrangement technique restreint des sections §2.4 et §4. Les constitutions de deux locataires s’accordent sur l’objectif délimité de la fédération ; les deux opérateurs signent le manifeste de fédération ; le flux de données est direct entre les deux locataires ; chacun peut révoquer à tout moment. Le manifeste de fédération lui-même est un enregistrement souverain — il comporte sa propre provenance, sa propre politique, sa propre chaîne de preuves et son propre cache de vérification.

L'infrastructure de fédération est fournie de bout en bout dans la plateforme : le modèle d'accord, le service d'accord, l'interface de routage, une interface utilisateur pour l'administrateur, un chemin d'accès au journal d'audit, ainsi qu'une matrice complète de tests négatifs couvrant les lectures limitées au périmètre, le blocage des écritures entre locataires, l'exhaustivité du journal d'audit, la discipline de citation, la mise en cache/l'obsolescence, les états de données dans les cas limites, les limites d'autorisation et les conflits d'espaces de noms. Les liaisons de fédération en direct entre des locataires indépendants sont en attente du premier déploiement multi-instances ; le modèle bilatéral est en place, mais les déploiements ne le sont pas. La section 7 décrit l'implémentation en détail.

5.6 Portabilité souveraine à l'initiative des membres

Un membre qui souhaite quitter son tenant — pour migrer vers un autre tenant fonctionnant selon le même modèle architectural, pour transférer son contenu vers une autre communauté, ou pour satisfaire au droit d'accès prévu à l'article 15 du RGPD — peut le faire via une exportation canonique. L'exportation contient tous les enregistrements dont le membre est l'auteur, le kaitiaki ou est autrement désigné comme personne concernée ; chaque enregistrement transmet sa chaîne de preuve ; la partie destinataire peut vérifier la chaîne par rapport au document DID publié par le locataire source sans faire confiance à aucun des deux opérateurs. Les enregistrements dont la politique interdit l'exportation (par exemple,

une délibération contribuée sous des conditions de consentement collectif) sont répertoriés dans le manifeste d'exportation comme retenus, avec mention de la raison liée à la politique.

Il s’agit du cadre architectural de l’article 15 du RGPD : non pas un point d’accès à usage spécifique, mais le même pipeline d’exportation que l’ architecture utilise pour tous les mouvements d’enregistrements souverains, instancié pour le cas de la personne concernée en tant que membre. La section 8 décrit la mise en œuvre, y compris le chemin d’ingestion du locataire destinataire qui boucle la migration .

---

6. Mise en œuvre architecturale

Cette section présente les composants qui concrétisent les principes de conception de la section 5 en code. Chacun est en production sur les deux sites d’infrastructure (OVH France, sous souveraineté de l’UE ; Catalyst Cloud, sous souveraineté de la Nouvelle-Zélande) et vérifiable à partir de la base de code et de l’interface API en fonctionnement. Conformément à la politique de périmètre IP (section 13), ce rapport décrit les composants architecturaux et leurs interactions plutôt que les chemins d’origine par fichier.

6.1 Primitive de provenance cryptographique

La primitive de provenance calcule le SHA-256 sur une sérialisation JSON canonique des champs obligatoires et facultatifs de l’origine. Le point d’entrée produit le hachage ; un vérificateur le recalcule et le compare au hachage stocké. L’identifiant de l’algorithme accompagne l’ enregistrement. Une aide à la forme canonique élimine l'énumération dépendante du mode d'hydratation — un mode de défaillance apparu lors de la validation des cas d'utilisation, où un sérialiseur itérant sur les propriétés énumérables d'un sous-document ORM produisait des hachages qui divergeaient selon les modes d'hydratation, alors qu'une suite d'unités de test substantielle sur des charges utiles d'objets simples passait sans problème. La correction a consisté en une seule étape de normalisation ; la discipline qui a permis de la mettre en évidence (validation des cas d'utilisation sur des bases de données en production, et non pas uniquement sur des tests simulés) fait désormais partie des normes opérationnelles du projet.

6.2 Signature de la chaîne de preuves lors des créations, mises à jour et suppressions

Chaque écriture dans un enregistrement marqué comme souverain ajoute une entrée signée à la chaîne de preuves de l’enregistrement. Les entrées CREATE sont signées par la clé de signature de preuve du locataire (fournie via le magasin de clés du locataire, §6.6) et lient l’entrée au hachage de provenance de l’enregistrement. Les entrées UPDATE sur les écritures en mode document ne sont émises que lorsque les chemins pertinents pour la souveraineté ont changé (à l'exclusion des champs de comptabilité tels que `updatedAt`) ; la liste des chemins modifiés est capturée. Les entrées UPDATE en mode requête suivent la même structure, calculée à partir de la différence entre les documents pré-image et post-image sur `updateOne`, `updateMany`, `findOneAndUpdate` et les chemins associés. Les croisements DELETE sont gérés par deux couches de hooks — un hook en mode document et un hook en mode requête couvrant les variantes unique, par lots et findAndDelete. Les deux couches produisent un enregistrement Tombstone contenant l'entrée de suppression signée comme preuve de la suppression ; les tombstones en mode requête se distinguent de manière observable des tombstones en mode document via le champ `policy_evaluated_by`. Un composant distinct étend cela au modèle de file d’attente de gouvernance, garantissant que les suppressions internes à la gouvernance laissent également une trace cryptographique signée.

6.3 Mise en cache de la vérification et intégration du chemin de lecture

La vérification de la chaîne de preuves s’effectue lors de l’ingestion et est mise en cache dans le bloc de cache de vérification de l’enregistrement : l’heure de la dernière vérification, le SHA-256 de la chaîne de preuves canonisée à ce moment-là, les algorithmes vérifiés et la prochaine date limite de revérification (par défaut 90 jours ; configurable par le locataire via la constitution). Le vérificateur expose trois points d'entrée : une vérification et une mise en cache au moment de l'ingestion, une vérification synchrone du cache au moment de la lecture, et un balayage par lots planifié.

Le câblage est uniforme. Un hook de pré-enregistrement calcule la provenance et signe l'entrée de création. Un hook de post-enregistrement déclenche la vérification et la mise en cache après chaque écriture, avec un délai de rebond via un ensemble de clés en vol pour éviter les conditions de tempête . Une tâche planifiée s'exécute quotidiennement sur les modèles de contenu générés par le locataire, traitant par lots les entrées de cache expirées. Le hook post-sauvegarde se déclenche lors des créations et des mises à jour pertinentes pour la souveraineté ; un filtre de liste de chemins exclut les chemins de comptabilité afin que les écritures du vérificateur lui-même ne déclenchent pas le hook en boucle ; les sauvegardes de comptabilité uniquement contournent le vérificateur et limitent le coût de la revérification aux véritables changements de souveraineté. Le chemin de lecture complète l'interface. Chaque réponse GET de l'API sur un enregistrement marqué de souveraineté comporte un champ de vérification : compact {valid, reason} sur les réponses de liste, et des informations détaillées supplémentaires (verified-at, re-verify) sur les réponses de type « tout afficher ».

Le chemin de lecture complète la surface. Chaque réponse GET de l'API sur un enregistrement marqué comme souverain comporte un champ de vérification : compact `{valid, reason}` sur les réponses de liste, extras détaillés (verified-at, re-verify-after, algorithms-verified) sur les réponses détaillées. L'implémentation est uniforme : un seul décorateur d'aide est invoqué à partir des chemins « lean » et « aggregate » de chaque route.

6.4 Moteur d’héritage des politiques et application au niveau du groupe

Le moteur d’héritage des politiques lit la constitution du locataire, les appartenances aux sous-groupes du membre demandeur, le bloc de politique de l’enregistrement et l’opération demandée (lecture/écriture/exportation/suppression). Il renvoie une politique effective avec des motifs de violation explicites lorsqu’une requête échoue. Trois options de filtrage restreignent l’accès conformément à la section 5.4.

L'application au niveau du groupe dépend des enregistrements portant un `collective_id` valide. Un assistant valide l'identifiant de sous-groupe fourni par l'appelant par rapport à trois contraintes (format, portée du locataire, appartenance du lecteur) et renvoie un contexte atomique — atomique car un `collective_id` sans `share_within: ['group']` est purement décoratif (la porte ne s'appliquerait pas). Huit chemins de création de contenu (Sondage, Événement, Article, Album, Délibération, Message de chat, Covoiturage, Ressource) acceptent l’identifiant de sous-groupe provenant du corps de la requête et le transmettent via l’assistant. La rétrocompatibilité est préservée : les appelants omettant le champ créent des enregistrements à la portée du locataire comme auparavant. Des sélecteurs d’interface utilisateur par formulaire exposent la sélection de sous-groupe au niveau du formulaire de création sur les huit interfaces.

Le mode strict de portée inconnue comble une faille de type « fail-open » présente dans les itérations antérieures. Un ensemble de valeurs de portée reconnues à l'échelle de la plateforme définit le vocabulaire ; toute valeur en dehors de cet ensemble est désormais refusée avec une raison nommée, à moins qu'une portée reconnue dans le même ensemble n'accorde déjà l'accès. Il s'agit de la position de principe du projet — *être honnête sur ce qui ne peut être vérifié ; ne pas inventer d'autorisation pour cela* — appliquée à la barrière du

chemin de lecture.

6.5 Éditeur de constitution souveraine La

La constitution souveraine d'un locataire est modifiable par l'administrateur du locataire via un parcours et une interface dédiés. L'éditeur expose les paramètres par défaut de la constitution (mode de résolution par défaut, mode d'exportation par défaut, autorité présumée par défaut, modèle de chiffrement), un tableau de catégories qui répertorie les modèles de contenu canoniques et permet la définition de catégories personnalisées par le locataire, ainsi qu'une prise en charge multilingue en anglais, allemand, français, néerlandais et te reo Māori. Les traductions en te reo Māori ont été réalisées à l'aide des outils de traduction du projet (DeepL, qui prend en charge le te reo Māori sous le code de langue `MI` — un fait régulièrement mal interprété par les commentateurs externes et corrigé au sein même du projet) et leur sens a été vérifié ponctuellement.

Une fenêtre de transition constitutionnelle signifie que les locataires modifiant leur constitution voient s'afficher une bannière indiquant que la modification ne devient contraignante qu'après la transition ; il s'agit du mécanisme de contrôle des prérequis constitutionnels qui distingue un projet de constitution d'une constitution contraignante. Une barrière distincte (la barrière de la constitution souveraine) applique strictement le code 403 aux locataires créés après la date de basculement qui ne disposent pas des sections souveraines requises, avec une immunité de suspension intégrée pour les locataires désignés de l'infrastructure de la plateforme .

6.6 Magasin de clés du locataire

Les clés de chiffrement et de signature de chaque locataire sont stockées dans un magasin de clés au niveau du locataire, avec des opérations de génération, de récupération, de rotation et de destruction. Les clés sont identifiées par des identifiants stockés dans le bloc de chiffrement de chaque enregistrement. La suppression cryptographique d'un enregistrement — régie par la politique via l'indicateur `delete_must_be_cryptographic` — s'effectue en détruisant la clé de chiffrement propre à l'enregistrement dans le magasin de clés du locataire, rendant le texte chiffré de l'enregistrement irrécupérable à partir de l'état persistant.

6.7 Publication décentralisée des identifiants

Les identifiants décentralisés des locataires et des membres suivent la spécification DID du W3C [11] et sont publiés sous le domaine du locataire (`/.well-known/did.json` pour le document DID du locataire ; `/.well-known/did/members/${slug}/did.json` en option pour les DID des membres). Les documents DID contiennent les méthodes de vérification du locataire utilisées pour signer les entrées de la chaîne de preuves ; un vérificateur externe détenant le document DID du locataire peut vérifier chaque entrée signée contenue dans un enregistrement, y compris les entrées des enregistrements exportés en vertu du §8 vers un autre locataire.

6.8 File d'attente de gouvernance

Le modèle de file d'attente de gouvernance couvre les cas nécessitant une décision du locataire-arbitre : violations de politique, demandes de résolution de conflits, demandes de suppression initiées par un membre et nécessitant l'approbation de la gouvernance. Les états du cycle de vie — créé → en cours d'examen → décidé → mis en œuvre (ou rejeté) — sont soumis à des conditions de transition ; chaque décision et chaque mise en œuvre laissent des entrées de piste signées que le locataire peut reconstituer à partir de sa propre base de

données. L'application des délais est automatiquement mise en œuvre conformément à la résolution par défaut constitutionnelle du locataire lorsqu'une entrée dépasse son délai de grâce.

6.9 Enveloppe d'exportation avec superposition de visibilité non administrative et journalisation d'audit symétrique

Chaque exportation d’enregistrement souverain passe par un wrapper qui s’applique sous trois conditions : chaque enregistrement comporte une provenance ; chaque enregistrement appartient au locataire demandeur ; le mode complet nécessite le rôle d’administrateur du locataire. Les modes hachage et agrégation sont désormais accessibles aux membres ordinaires via une superposition de visibilité qui filtre les enregistrements en fonction de l’horizon de lecture de l’appelant avant de produire la projection — contournement du propriétaire ; règles par niveau de visibilité ; sécurité intégrée en cas d’erreurs de préchargement de sous-groupes. Les violations génèrent une entrée dans le journal d’audit de gouvernance accompagnée d’une justification. Les exportations réussies génèrent également une entrée d’audit contenant le mode de capture des métadonnées (complet/hachage/agrégé), le nombre d’enregistrements avant et après filtrage, la ventilation par modèle et l’identité de l’appelant. Chaque exportation — réussie ou non conforme — est reconstituable à partir du journal d’audit ; aucune exportation n’est silencieuse.

6.10 Migration uniforme des enregistrements souverains à travers les modèles de contenu générés par les locataires

Le bloc de métadonnées des enregistrements souverains est appliqué de manière uniforme à l’ensemble des modèles de contenu générés par les locataires. La migration a été différée lorsque cela était possible (les enregistrements acquièrent les métadonnées lors de la première écriture sous le nouveau schéma) et immédiate lorsque cela était nécessaire (un script unique a renseigné la provenance pour le stock d’enregistrements existant). Le même bloc de métadonnées s’étend aux surfaces de sous-documents intégrés (EventMenu, Edition et similaires) sous une extension de plugin uniforme. Le cache de vérification est renseigné sur l’ensemble des locataires opérationnels des deux sites de production ; le petit résidu d’enregistrements hérités sans hachage de provenance est marqué `comme « non vérifiable »` plutôt que « `valide` » — le choix architectural consiste à faire apparaître ce qui ne peut être vérifié plutôt que de synthétiser un cache pour cela.

6.11 Alignement des politiques des workers et des WebSockets

La couche de travailleurs asynchrones applique la politique constitutionnelle du locataire aux enregistrements qu’elle crée. Les deux travailleurs de la chaîne de création concernés (traitement des e-mails en contenu ; numérisation de documents) font appel à un assistant partagé qui assemble un contexte de politique à partir des métadonnées de la tâche d’origine (identifiant du locataire ; identifiant du membre d’origine ; identifiant du sous-groupe d’origine le cas échéant) et définit `les propriétés metadata.origin` et `metadata.policy` sur l’ enregistrement au moment de sa création. Les workers qui mettent à jour des enregistrements souverains existants (enrichissement OCR des contributions téléchargées ; amélioration des médias ; extraction d’histoires ; validation vocale) conservent la politique définie en amont au moment de la création et n’ont pas besoin de l’assistant. Les workers qui ne produisent aucun contenu souverain (coordination de l’orchestrateur ; numérisation de la file d’attente ; pipelines de transcription qui modifient les enregistrements de la file d’attente opérationnelle) ont été audités dans le cadre de cette étude et il a été confirmé qu’ils n’avaient pas besoin de l’assistant. L'interface WebSocket est reliée au même calcul de politique effective via un filtre de diffusion par destinataire ; avant qu'un message de chat n'atteigne une socket de destinataire, le prédicat de visibilité est évalué pour cette socket,

et le message est omis si la vérification de visibilité échoue. Les diffusions de fédération passent sans modification — la visibilité de la fédération est décidée au niveau du service de fédération, et non au niveau de la diffusion.

6.12 Primitive de compaction de la chaîne de preuves Une

Une primitive de compactage de la chaîne de preuve remplace une sous-plage contiguë de la chaîne de preuve d'un enregistrement par une seule entrée de résumé signée dont la charge utile est le SHA-256 du JSON canonique de la sous-chaîne remplacée. La vérification d'une entrée compactée s'effectue selon deux modes : un mode par défaut peu coûteux traite l'entrée compactée comme une seule étape signée, ancrée par le hachage de résumé ; un mode complet récupère la sous-chaîne archivée avant compactage et vérifie entrée par entrée. La primitive est activable par configuration du locataire ; elle est désactivée par défaut. Son application aux chaînes de preuves des locataires en production est gérée par l'opérateur.

6.13 Mise à niveau des tombstones

Une primitive de mise à niveau des tombstones signe les tombstones en texte clair préexistants, datant d'avant l'introduction de la signature des chaînes de preuve, afin que la piste d'audit soit uniforme sur l'ensemble de l'historique du locataire. La mise à niveau s'effectue par locataire, de manière idempotente et reprenable, et ajoute une entrée signée à côté des champs en texte clair d'origine sans les effacer. La primitive est gérée par l'opérateur ; aucune tombstone de locataire en production n'a encore été mise à niveau.

6.14 Consultation du cadre en tant que piste d'audit

Chaque décision architecturale dans le développement de la plateforme est précédée d'une consultation du cadre : un compte rendu de décision documenté mentionnant les services consultés, la liste des conditions par service et le verdict. Les consultations sont enregistrées dans des bases de données de production locales ainsi que dans des bases de données relevant de la souveraineté de l'UE et de la Nouvelle-Zélande. L'enregistrement est automatisé par des scripts par décision ; le format documentaire est un fichier Markdown par décision situé dans `le répertoire docs/framework-consultations/.` La rigueur de l' enregistrement — trois emplacements d'insertion par consultation afin qu'aucune perte sur un seul hôte ne compromette la traçabilité — constitue la contribution ; la valeur réside dans la reproductibilité et l'auditabilité, et non dans le nombre d'enregistrements.

Il ne s'agit pas d'une démonstration de vertu. La consultation est le mécanisme du projet permettant de lier les décisions architecturales à des artefacts observables : un futur lecteur pourra se demander *quelles conditions l'intégration du chemin de lecture a-t-elle traitées ?*, et la réponse se trouve dans la base de données. Le document de travail du cadre Tractatus [1] documente le modèle du point de vue du cadre ; cet article documente une instance de celui-ci du point de vue de la plateforme, le registre des consultations faisant partie de la surface d'évaluation (§12).

---

7. Fédération bilatérale en production

Le modèle de fédération bilatérale est construit de bout en bout, avec une surface de vérification substantielle ; les liens de fédération en direct entre des déploiements de locataires indépendants restent en attente. L'architecture est prête pour le premier déploiement multi-instances ; les déploiements ne sont pas encore établis.

7.1 Le manifeste de fédération

Une fédération entre deux locataires souverains se matérialise sous la forme d'un enregistrement d'accord de fédération signé par les deux locataires. L'accord précise l'objectif délimité (mise en relation pour le covoiturage, annonce d'événements partagés, délibération conjointe, cogestion de kaupapa, référence interdomaines des programmes d'études), la forme du flux de données (quels champs traversent quelle voie, quelle transformation, quelle conservation de chaque côté), la résolution des politiques inter-locataires (quelle constitution régit les enregistrements créés dans le cadre de la fédération ; comment les conflits de politiques sont résolus), la procédure de révocation (chaque partie peut révoquer unilatéralement ; la révocation est un enregistrement signé ; la propagation est immédiate), et la conservation des audits (chaque locataire conserve une copie signée de chaque interaction inter-locataires).

Le manifeste est lui-même un enregistrement souverain. Une fédération ne peut s'activer sans signatures vérifiées des deux parties par rapport à leurs documents DID respectifs. L'annexe C présente la structure du schéma au niveau des composants architecturaux ; les détails spécifiques des champs de mise en œuvre sont conservés conformément à la posture du périmètre IP (§13).

7.2 Interface utilisateur de l'administrateur et journal d'audit

Un administrateur de locataire gère les accords de fédération via une interface utilisateur dédiée qui affiche le cycle de vie de la fédération (proposé → accepté → actif → révoqué) et expose le journal d'audit. Chaque événement transfrontalier — une proposition de fédération, une acceptation, une requête acheminée à travers la fédération, une révocation — laisse une entrée signée dans le journal d'audit de la fédération. Le journal d'audit peut être reconstitué de chaque côté indépendamment ; aucun locataire ne s'appuie sur la tenue des registres de l'autre pour sa propre position d'audit.

7.3 Matrice de tests négatifs

Une matrice de tests négatifs (sous couverture d'intégration continue) vérifie les invariants de la surface de la fédération. Douze catégories sont structurées : lectures liées à la portée (y compris une vérification statique qu'aucune référence de collection interdite n'apparaît dans le code du service de fédération), blocage des écritures inter-locataires, exhaustivité du journal d'audit, discipline de citation, comportement de mise en cache/obsolescence, états de données dans les cas limites (champs manquants ; distinction entre null et absent), application des limites d'autorisation et résolution des conflits d'espaces de noms de phase 3. Un sous-ensemble de la matrice est parcouru par un validateur multi-locataires en direct qui exécute la pile HTTP complète sur un déploiement en cours d'exécution ; le reste est exécuté sur un dispositif au niveau du service ou sous forme d'assertions statiques de grep de code.

Le test le plus exigeant de la matrice est une assertion statique : le fichier du service de fédération est lu sous forme de texte, les commentaires sont supprimés, et les noms de collections interdits sont comparés au code exécutable. L' assertion est codée sous forme de test par CI, et non de vérification ponctuelle avant validation ; tout élargissement futur de la surface de lecture de la fédération introduisant une référence à une collection interdite fait échouer l'assertion au moment de la CI.

7.4 État du déploiement en production

Les liens de fédération en production entre des locataires indépendants sont en attente du premier déploiement multi-instances. La fédération de covoiturage — une catégorie de fédération reliant un ensemble de communautés pour la mise en relation de covoiturage

exclusivement sur Koha — est le déploiement multi-instances cible initial. Un locataire de covoiturage est en cours de développement sur une infrastructure souveraine néo-zélandaise (Catalyst Cloud) ; la fédération multi-instances s'active dès qu'au moins deux locataires de covoiturage sont opérationnels. **Les communautés ou organisations qui envisagent le déploiement multi-instances du covoiturage comme alternative à une infrastructure souveraine — praticiens des transports communautaires, chercheurs en équité des transports, programmes de résilience rurale, groupes universitaires sur la durabilité ou les transports — sont invités à contacter l'auteur correspondant concernant la participation au projet pilote.** Les déploiements de fédération d'iwi à iwi — où un iwi partage du matériel kaupapa spécifique avec un autre, par le biais d'un manifeste signé, tout en conservant le contrôle total de la révocation — sont soutenus sur le plan infrastructurel mais dirigés par les opérateurs ; aucune fédération d'iwi à iwi active n'avait été mise en place au moment de la rédaction de ce projet.

Le cadre de la fédération bilatérale défini au §5.5 est donc un *engagement architectural avec une infrastructure livrée et une surface de vérification*, et non un *réseau déployé de fédérations actives*. La propriété architecturale en jeu — à savoir que deux communautés peuvent convenir, selon des conditions qu'elles spécifient, d'une interaction délimitée spécifique, et uniquement celle-ci — est exactement ce que les trois articles du Te Tiriti impliquent pour l'infrastructure numérique : la souveraineté tribale sur les taonga est respectée car chaque iwi conserve l'autorité totale au sein de son propre tenant, et la fédération n'érode pas cette autorité — elle permet une interaction délimitée spécifique dans le cadre de l'architecture.

---

8. Portabilité souveraine — Intégration DSR

Le sixième engagement de conception de l'architecture (§5.6) est qu'un membre est un sujet de données de premier ordre. Un membre qui souhaite quitter son tenant — pour migrer vers un autre tenant sous le même modèle architectural, pour transférer ses données vers une autre communauté, ou pour satisfaire un droit des personnes concernées au titre du RGPD — peut le faire via une exportation canonique.

8.1 Le paquet d'exportation canonique —

Une exportation canonique initiée par un membre contient tous les enregistrements dans lesquels le membre est l'auteur, le kaitiaki ou désigné d'une autre manière comme personne concernée. L'exportation est un ensemble paginé couvrant les modèles de contenu générés par le tenant et marqués de manière souveraine, y compris les surfaces intégrées le cas échéant. Chaque enregistrement du paquet comporte sa chaîne de preuve complète, son bloc de politique complet et son hachage de provenance. Le manifeste du paquet est lui-même signé par le locataire source ; un vérificateur externe détenant le document DID du locataire source peut vérifier chaque entrée signée du paquet sans faire confiance à aucun des deux opérateurs. Le paquet est rendu au format JSON, CSV ou PDF selon le format de la requête ; le contenu canonique sous-jacent est identique dans tous les rendus.

8.2 Exportation respectueuse des politiques et manifeste de la liste des éléments retenus

Le wrapper d'exportation applique la politique. Les enregistrements dont la politique interdit l'exportation (par exemple, une délibération contribuée sous des conditions de consentement collectif ; un élément multimédia soumis à une contrainte de partage spécifique au tikanga) sont répertoriés dans le manifeste d'exportation comme retenus, avec mention de la raison politique. Le membre reçoit à la fois le lot et la liste des éléments retenus ; la liste

des éléments retenus est elle-même signée, de sorte que le membre dispose d'un artefact vérifiable attestant de ce qui a été exclu et pourquoi. La discipline consiste en une divulgation complète de ce qui est retenu et pourquoi : toute tentative d'utiliser un droit de la personne concernée comme prétexte pour accéder à des données auxquelles le membre n'a aucun droit légitime se heurte au filtre de la politique, et la réponse elle-même est vérifiable.

Le mécanisme de la liste des données non divulguées est la réponse architecturale à une tension que les régulateurs identifient depuis des années : le droit d'accès prévu à l'article 15 est limité par les droits d'autres personnes identifiables (article 15, paragraphe 4) et par d'autres motifs de traitement légitimes. Une implémentation standard peut soit renvoyer tout (en violant les droits des autres parties), soit renvoyer moins que ce qui a été demandé (sans expliquer le motif de l'exclusion). La position de l'architecture est que chaque enregistrement exclu est nommé, que la raison politique est citée, et que le manifeste liant ces deux éléments est vérifiable.

8.3 Ingestion par le locataire destinataire (migration inter-locataires)

Un membre peut transférer son ensemble d'exportation canonique vers un autre locataire fonctionnant selon le même modèle architectural. Le chemin d'importation du locataire destinataire vérifie la chaîne de preuve de chaque enregistrement par rapport au document DID du locataire source, accepte les enregistrements (lorsque la constitution du locataire destinataire le permet) et poursuit la chaîne de preuve — le locataire destinataire signe une entrée `ingest_via_migration` sur chaque enregistrement, en indiquant le nom du locataire source et le hachage du manifeste du paquet. L' identité du membre est établie par son DID inter-locataires ; la migration est enregistrée des deux côtés comme un événement normal de registre souverain. Une vérification de la conformité constitutionnelle du locataire destinataire est obligatoire, et non facultative : les enregistrements dont la politique du locataire source est incompatible avec les paramètres par défaut du locataire destinataire (par exemple, une politique de confidentialité plus stricte refusant une politique d'expéditeur plus permissive) sont répertoriés comme REJETÉS avec la raison de la politique. L'accusé de réception du paquet migré est signé par le locataire destinataire et renvoyé au membre, fournissant une clôture vérifiable à la migration.

La mise en œuvre actuelle du chemin d'ingestion du locataire destinataire couvre les phases A à F : résolution du DID source, vérification du paquet, vérification de la conformité, ingestion avec continuation de la chaîne de preuves, signature de l'accusé de réception et scénarios de tests d'intégration de bout en bout consultés par le cadre. La réconciliation d'identité dans l'implémentation v1 est configurée pour refuser l'intégration automatique par défaut — un membre migrant doit déjà être membre du locataire destinataire, ou l'administrateur du locataire destinataire doit approuver manuellement la création de l'adhésion avant l'ingestion du paquet. Il s'agit d'un choix délibérément prudent : l'intégration automatique via un DID inter-locataires présente une surface de sécurité qui justifie sa propre phase de conception, et l'implémentation v1 la reporte.

8.4 Articles 15, 16, 17, 18, 20 et 21 du RGPD

L'interface de l'endpoint DSR met en œuvre l'ensemble des six droits des personnes concernées prévus par le RGPD via le même pipeline d'exportation, avec des comportements spécifiques à chaque droit lorsque cela est nécessaire :

- **Article 15 (Droit d'accès) :** l'exportation canonique, telle que décrite aux §8.1–§8.2.
- **Article 16 (Droit de rectification) :** les membres peuvent demander une correction ; la demande est soumise à des conditions de politique ; les corrections acceptées laissent une entrée signée dans la chaîne de preuve.

- **Article 17 (Droit à l'effacement) :** les enregistrements rédigés uniquement par le membre, lorsqu'aucun autre droit n'est en jeu, peuvent être supprimés de manière cryptographique sur demande — la clé de chiffrement par enregistrement est détruite dans le magasin de clés du locataire ; le texte chiffré devient irrécupérable ; une marque d'effacement signée consigne la suppression. Les enregistrements impliquant d'autres parties (un commentaire sur l'histoire d'un autre membre ; une contribution à une délibération multi-auteurs) suivent la règle par défaut prévue par la constitution pour l' effacement par consentement collectif — la file d'attente de gouvernance du locataire reçoit la demande, les parties concernées sont consultées conformément au processus du locataire, et la décision qui en résulte est mise en œuvre avec une piste d'audit complète.
- **Article 18 (Droit à la limitation) :** la limitation est mise en œuvre sous la forme d'une dérogation à la politique qui empêche le traitement tant que la demande est en attente ; la dérogation est elle-même un événement souverain.
- **Article 20 (Droit à la portabilité des données) :** l' ensemble canonique de la section 8.1, avec le chemin d'ingestion du locataire destinataire de la section 8.3 comme achèvement architectural.
- **Article 21 (Droit d'opposition) :** l'opposition est consignée dans l'enregistrement concerné et se propage à travers la passerelle de politique sous la forme d'un veto de traitement par enregistrement.

Le délai de réponse de 30 jours prévu à l'article 15 est appliqué par un minuteur de journal d'audit ; les réponses manquées déclenchent une alerte dans la file d'attente de gouvernance du tenant.

8.5 La tension avec les exceptions de l'article 17

Le cadre architectural de la tension relative au droit à l'effacement entre l'article 17 et les exceptions de l'article 17(3) (liberté d'expression ; actions en justice) ne signifie pas que cette tension n'existe pas ; la tension est réelle. L'architecture définit explicitement la résolution, dans la constitution du locataire, avec une mise en œuvre soumise à des politiques et une piste d'audit complète. La demande d'effacement d'un membre est honorée dans la mesure où la résolution constitutionnelle le permet ; lorsque les conditions de consentement collectif exigent un processus multipartite, celui-ci est consigné et la décision qui en résulte (effacer, expurger, conserver) est signée. Un auditeur externe consultant le journal d'audit peut déterminer exactement quelle exception à l'article 17 a été invoquée, par qui, sur quel enregistrement et avec quel résultat.

---

9. Interface utilisateur de gouvernance des parties prenantes

L'interface utilisateur de gouvernance expose la posture constitutionnelle de la plateforme, la discipline de communication, l'historique des décisions, le registre de consultation du cadre, l'espace de dialogue et l'espace d'examen par les parties prenantes. Il s'agit d'une interface destinée aux parties prenantes, délibérément conçue pour être lisible par les trésoriers de paroisse et les anciens de la communauté plutôt que par les seuls ingénieurs. L'interface utilisateur se trouve sur un sous-domaine de locataire dédié au centre d'opérations et est répliquée sur chaque sous-domaine de locataire selon un modèle uniforme. Les phases 1 à 7 sont disponibles à la date de publication du présent document ; la phase 6 (dialogue participatif) et la phase 7 (généralisation inter-types de produits) étendent l'interface de l' examen en lecture seule à la gouvernance participative.

Deux modèles d'engagement des parties prenantes traversent l'interface. Le premier est **l'invitation**: un administrateur de tenant émet une invitation signée à l'intention d'une partie

prenante, précisant le nom de la partie invitée, les interfaces qui lui sont ouvertes et la date d'expiration de l'invitation ; la partie prenante accepte via une URL à usage unique ; la session qui en résulte est soumise aux mêmes règles d'accès qu'une session de membre, l'horizon de lecture étant limité aux interfaces auxquelles elle a été invitée. Le second est **la demande**: lorsqu'une partie prenante sollicite un accès sans invitation préalable, la plateforme achemine la demande vers la procédure propre au locataire définie dans la constitution de ce dernier. Les éléments architecturaux de base — émission d'invitation, jeton d'acceptation, piste d'audit signée — sont uniformes entre les locataires et sont décrits dans les sous-sections ci-dessous ; la procédure de demande initiée par la partie prenante est définie par la constitution de chaque instance de Village et n'est pas spécifiée dans le présent document. Les constitutions de référence fournies par la plateforme sont documentées dans la visionneuse de constitution (§9.1) mais ne sont pas normatives.

9.1 Visualiseur de constitution (Phase 1)

La visionneuse de constitution affiche l'agrégation stable et ancrée de la plateforme destinée aux parties prenantes, issue des trois sources principales (les règles strictes du projet, les éléments de mémoire jamais tronqués et les principes universels de la plateforme de couche 1). Le rendu suit un modèle de chargement de page Markdown : pas de route API, pas de récupération dynamique, la visionneuse est un fichier HTML statique qui charge le Markdown via HTTPS et le rend. Ce modèle est intentionnel : la visionneuse est l'artefact le plus simple possible, vérifiable par tout réviseur capable de lire le HTML et le Markdown.

9.2 Visualiseur de la Constitution des communications (Phase 2)

La visionneuse de la Constitution des communications suit le même modèle, exposant le règlement de communication destiné aux opérateurs (pile de canaux, cadence, lignes de refus, règles « brouillons uniquement, ne jamais envoyer »). La version actuellement publiée clôt les éléments soumis par les opérateurs sous la responsabilité de l'agent délégué par l'opérateur selon son meilleur jugement ; les révisions ultérieures attendent l'approbation de l'opérateur.

9.3 Visualiseur du journal des décisions (Phase 2)

La visionneuse du journal des décisions présente un index organisé des décisions importantes prises tout au long du développement de l'architecture (primitives architecturales, position des fournisseurs, règles de confidentialité et de contenu, discipline des processus, formation et IA). La visionneuse de la Constitution et la visionneuse de la Constitution des communications renvoient toutes deux à la visionneuse du journal des décisions dans leurs sections « Companions ». L'arc complet lisible par les parties prenantes — Constitution → Constitution des communications → Journal des décisions — est accessible sur chaque sous-domaine de locataire .

9.4 Visualiseur de consultation du cadre (Phase 3)

La visionneuse de consultation du cadre expose le registre de consultation via une interface HTML accessible aux parties prenantes. La visionneuse présente un index agrégé par référence de document (une ligne par décision architecturale, avec les services consultés, les conditions, les verdicts et les dates) et une vue détaillée par décision exposant la liste complète des conditions par service et la piste des verdicts . La visionneuse est en lecture seule ; le registre sous-jacent est alimenté par les scripts d'enregistrement automatisés des consultations de la plateforme ; les parties prenantes lisent mais n'écrivent pas.

9.5 Accès par jeton d'invité pour les parties prenantes (Phase 4)

Une session d’invité spécifique à une partie prenante accorde un accès en lecture seule à l’ interface utilisateur de gouvernance sans nécessiter d’enregistrement complet en tant que membre du tenant. Un administrateur de la plateforme émet une invitation à la partie prenante ; l’invitation est un enregistrement signé mentionnant le nom de la partie prenante, les surfaces invitées et la date d’expiration de l’invitation ; la partie prenante accepte via une URL à usage unique ; la session qui en résulte présente la même posture de contrôle d’accès que la session d’un membre, mais avec un horizon de lecture limité aux surfaces invitées.

La propriété architecturale est que l'examen par les parties prenantes est lui-même une interaction avec des enregistrements souverains : chaque invitation, chaque acceptation, chaque lecture est consignée, signée et reconstituable à partir de la piste d'audit. Un bailleur de fonds ou un évaluateur de politique ayant examiné l'interface utilisateur de gouvernance de la plateforme peut produire un enregistrement vérifiable de ce qu'il a examiné, quand et par rapport à quelle version du matériel sous-jacent.

9.6 Interface d’examen par les parties prenantes (Phase 5)

Une interface de révision finale regroupe les documents de l’interface utilisateur de gouvernance en un index unique et navigable destiné aux parties prenantes : une page unique qui répertorie chaque article de la Constitution, chaque entrée du journal des décisions, chaque règle de la Constitution des communications et chaque consultation récente sur le cadre, avec des liens profonds vers chacun d’entre eux. Cette interface est le point d’arrivée naturel d’une invitation de phase 4 ; une partie prenante qui accepte l’invitation accède à l’interface de révision et peut naviguer à partir de là.

9.7 Dialogue participatif (Phase 6)

La surface de dialogue de la phase 6 transforme l’interface utilisateur de gouvernance en lecture seule en une interface participative. Les parties prenantes peuvent commenter les articles de la Constitution, les entrées du journal des décisions et les règles de la Constitution des communications ; les commentaires constituent eux-mêmes des enregistrements souverains, auxquels s’appliquent les mêmes mécanismes de provenance, de politique, de chaîne de preuve et de cache de vérification. La couche de langage situé de la plateforme répond aux requêtes des parties prenantes à partir du corpus curaté que l'interface utilisateur de gouvernance elle-même maintient, ce corpus servant de surface de citation. La défense contre les hallucinations est multicouche : une invite système renforcée oriente le modèle linguistique vers un refus par défaut pour les requêtes hors du corpus, et un filtre de discipline de citation rejette les réponses qui ne citent pas une source du corpus.

9.8 Généralisation inter-types de produits (Phase 7)

La phase 7 généralise la surface de dialogue de la phase 6 à l’ensemble des types de produits de la plateforme. Chaque type de produit possède ses propres chemins d’accès au corpus de dialogue, son vocabulaire et ses modèles de citation. La phase 7.A assure la généralisation par type de produit ; la phase 7.B construit le corpus de dialogue à modèles universels partagés ; la phase 7.C relie la surface d'affichage des commentaires approuvés en ligne à travers les pages de la visionneuse mdsl à l'aide d'ancres dynamiques et d'une API publique de widgets ; La phase 7.D constitue l’interface de fédération pour la couche de dialogue, qui utilise la même infrastructure de fédération bilatérale décrite au §7 (la matrice de test négatif est partagée, et non distincte ; la fédération des commentaires des parties prenantes entre villages est une application spécifique du modèle bilatéral général) ; la phase 7.E enregistre la règle de constitution des communications et la ligne du registre qui documente l’adoption de l’interface. L’effet cumulatif des phases 1 à 7 est une interface de gouvernance des parties

prenantes lisible, vérifiable, navigable, participative, sensible à la fédération et appliquée de manière uniforme à l’ensemble de la plateforme.

L'effet cumulatif des phases 1 à 7 est une surface de gouvernance des parties prenantes qui est lisible, vérifiable, navigable, participative, sensible à la fédération et appliquée de manière uniforme à tous les types de produits de la plateforme — au prix d’une surface de vérification substantielle (la matrice de test négatif de fédération bilatérale étant le plus grand contributeur individuel) et de la charge de travail liée à l’exécution de l’ enregistrement de consultation du cadre sur chaque extension architecturale.

---

10. Exemple concret : souveraineté de nommage interdomaines entre deux modules linguistiques situés

Cette section illustre le modèle de fédération bilatérale à l’aide d’un exemple concret, fourni par l’auteur correspondant à partir de ses travaux en cours de conception de programmes scolaires. L’exemple concerne l’intégration des programmes dans un contexte d’école primaire, mais le modèle architectural s’applique de manière générale à toute paire de communautés dont les positions en matière de souveraineté des données se recoupent en un point spécifique d’autorité interdomaines. Une présentation distincte est disponible dans le type de village « carpool » mentionné au §11 : « carpool » isole la primitive de fédération de la surface plus large orientée vers les membres des autres types de villages et constitue le cas minimal dans lequel le comportement de fédération du modèle peut être examiné de manière isolée. Le présent exemple pratique illustre la fédération entre deux domaines portant un contenu faisant autorité distinct ; la présentation « carpool » illustre la fédération entre deux instances du même type de village.

10.1 La configuration

Considérons deux modules linguistiques situés, chacun fonctionnant comme un locataire souverain sur la plateforme :

- **Un module de connaissances botaniques** pour une flore régionale — par exemple, un module « Flore de Nouvelle-Galles du Sud », détenu par une institution botanique responsable de la taxonomie validée, des noms scientifiques, de la distribution, des notes écologiques et des références croisées vers des sources scientifiques. Les propriétaires du module assurent la maintenance du contenu dans le cadre d’un processus d’amélioration continue : les nouvelles découvertes sont validées et intégrées ; les corrections sont publiées sous l’autorité signataire ; le corpus est la source faisant autorité en matière de référence botanique dans le cadre du champ d’application du module.
- **Un module de revitalisation linguistique** pour une langue autochtone de la même région — par exemple, un module « Langues aborigènes de Nouvelle-Galles du Sud », géré par une autorité linguistique communautaire chargée de valider le lexique, la prononciation, l’étymologie, le contexte culturel et le travail de revitalisation en cours. Les propriétaires du module conservent l’autorité sur la langue et ses usages, y compris la manière dont la langue nomme les entités du monde naturel.

Un point de convergence entre les domaines apparaît lors *de* la *dénomination des plantes*. Chaque plante du module botanique peut porter — en plus de son nom scientifique — un nom autochtone issu du lexique du module linguistique. Historiquement, ces noms autochtones relevaient du contrôle du module botanique en tant qu’annexes bibliographiques. Une décision politique visant à restaurer la souveraineté linguistique transfère l’autorité de dénomination du module botanique au module linguistique : désormais, le nom autochtone canonique d’une plante est celui que le module linguistique désigne comme tel.

10.2 La fédération comme solution architecturale

La réponse architecturale est une fédération bilatérale entre les deux modules, avec un manifeste qui définit précisément l'interaction délimitée :

- **Objectif délimité :** référence de nommage interdomaines. Le module botanique peut interroger le module linguistique pour obtenir le nom autochtone canonique d'une plante, à partir d'un nom binomial scientifique. Le module linguistique conserve toute autorité sur le nom ; le module botanique conserve toute autorité sur la taxonomie scientifique.
- **Flux de données :** une requête structurée émanant du module botanique et adressée au module linguistique identifie le nom binomial scientifique ; la réponse est le nom autochtone canonique (ou « `inconnu` » si le corpus du module linguistique ne répertorie pas encore cette plante). Le flux est *de type « pull-on-demand »*; aucun transfert par lots n'est prévu. Le module botanique peut mettre en cache les réponses avec une durée d'expiration configurable par le locataire.
- **Résolution des règles :** la constitution du module linguistique régit la réponse. Si le corpus du module linguistique est en cours de révision et qu'un nom est provisoirement en attente, la réponse indique ce statut dans un champ `caveats_added` de l'entrée de la chaîne de preuve ; le module botanique communique ce statut à ses utilisateurs.
- **Révocation :** l'une ou l'autre des parties peut révoquer à tout moment. La révocation se propage immédiatement ; le module botanique cesse d'interroger ; les réponses mises en cache expirent selon leur date d'expiration. Aucun flux de données ne se poursuit après la révocation.
- **Audit :** chaque requête et chaque réponse laissent une entrée signée dans la chaîne de preuves des deux côtés. Chaque partie peut reconstituer l'historique complet de la fédération à partir de sa propre base de données.

10.3 L'expérience de l'étudiant

Un étudiant suivant le programme pose une question : *« Quel est le nom autochtone de l'Eucalyptus camaldulensis ? »* Le parcours pédagogique de la plateforme achemine la requête vers le module botanique (qui contient le nom binomial scientifique en tant que source faisant autorité) et la fédération transmet la sous-requête de résolution de nom au module linguistique. La réponse est *élaborée à partir d'une combinaison de modules linguistiques contextualisés, et non à partir d'un grand modèle linguistique de pointe.* L' étudiant voit le nom, la référence du module linguistique et une indication que la réponse est fournie par la fédération — non pas parce que la fédération présente un intérêt technique pour l'étudiant, mais parce que la vérifiabilité est une valeur du programme d'études.

La propriété architecturale en jeu est que l'étudiant obtient une réponse faisant autorité et sélectionnée sans qu'un LLM n'intervienne. L'hallucination est structurellement exclue car aucun modèle ne génère la réponse à partir d'une distribution de probabilité sur des données d'entraînement ; la réponse est une requête fédérée sur un corpus sélectionné et géré par le détenteur des droits. Lorsque le corpus ne contient pas de réponse, la fédération renvoie «`inconnu` » — l'étudiant est informé que le système ne sait pas, une réponse structurellement exacte qu'une confabulation confiante d'un modèle de pointe ne peut offrir.

10.4 Les enseignements architecturaux

Trois leçons peuvent être tirées de cet exemple concret et répercutées sur les engagements architecturaux de la section 5 :

1. **Le transfert de souveraineté entre domaines est une opération de fédération.** Lorsque l'autorité sur une classe de références passe d'une communauté à une autre (module botanique → module linguistique sur la dénomination des plantes ; iwi → kāhui

sur un kaupapa partagé ; paroisse → diocèse sur un calendrier d'événements partagé), l'opération architecturale consiste à signer un nouveau manifeste de fédération, et non à migrer des données entre les locataires. Les données restent là où se trouve le titulaire des droits ; la fédération indique au consommateur où effectuer sa requête.

2. **La diffusion de programmes d'études via des modules fédérés situés est un déploiement structurellement distinct des réponses organisées par les LLM.** Le cas d'utilisation de la diffusion de programmes d'études est un puissant facteur empirique justifiant le parti pris de l'architecture contre la diffusion de contenu médiatisée par les LLM : lorsque l' étudiant est un apprenant, la réponse doit être faisant autorité, et non probabiliste.
3. **Le champ « bounded-purpose » du manifeste de fédération est portant.** Une fédération de résolution de noms n’autorise pas le module botanique à interroger l’ensemble du corpus du module linguistique ; elle n’autorise que la forme de requête spécifiée. Le service de fédération de la plateforme refuse les requêtes ne correspondant pas à la forme indiquée dans le manifeste. C’est la propriété architecturale qui permet à deux communautés souveraines de se fédérer autour d’une interaction spécifique et délimitée sans céder leur autorité sur rien d’autre.

Une gamme de classes de fédération connexes — entre le module de collection d’un musée et le module de biens culturels d’une communauté autochtone ; entre le module de planification d’un conseil régional et le module de site patrimonial d’un hapū ; entre le module de programme scolaire d’un district scolaire et le module de langue communautaire — partagent la même structure. L’exemple Flora ↔ Langues est proposé comme illustration canonique car il rend visibles simultanément les dimensions *de la souveraineté des données* et *du transfert d’autorité épistémique*.

---

11. Six configurations de type « village » — exemples tirés d’une famille de modèles

L'architecture s'exprime à travers un modèle de gabarit. Une configuration de locataire n'est pas une construction ponctuelle ; il s'agit d'une instanciation de gabarit, où le gabarit définit les primitives d'enregistrement souverain, le comportement d'héritage des politiques, la sémantique de fédération, l'interface utilisateur de gouvernance des parties prenantes , la forme de la file d'attente de gouvernance, tandis que la configuration spécifique au locataire définit ce que le modèle laisse ouvert : la constitution, la structure d'adhésion, la topologie des sous-groupes, les paramètres régionaux multilingues, la cohorte de couches linguistiques situées, les préférences des fournisseurs dans les limites de l' enveloppe d'interdiction des fournisseurs.

La valeur opérationnelle du modèle de gabarit réside dans le fait qu’une nouvelle configuration de type « village » est un exercice de configuration, et non une reconstruction. La valeur architecturale réside dans le fait qu’un réviseur examinant une configuration de type « village » examine *la même architecture* que celle sur laquelle toutes les autres configurations de type « village » fonctionnent également ; les propriétés de souveraineté sont uniformes au sein de la famille car le gabarit est uniforme.

La plateforme présentée dans cet article est elle-même l’implémentation de référence de l’architecture qu’elle décrit. La plateforme a été construite par une petite équipe en Nouvelle-Zélande, sous des contraintes d’interdiction des fournisseurs et de souveraineté — les mêmes contraintes contre lesquelles l’architecture se défend. La construction dans le cadre de ces contraintes a mis en évidence les modes de défaillance contre lesquels l’architecture se défend, y compris la tentation, sous la pression des coûts, de se rabattre sur une infrastructure relevant de la juridiction américaine pour le stockage ou le calcul. La

résistance de l’architecture à cette tentation, observée pendant la construction, est en soi une contribution documentée dans cet article.

La famille de modèles est opérationnelle : des configurations de type « village » fonctionnent sur une infrastructure relevant de la souveraineté de l’UE (OVH France) et sur une infrastructure relevant de la souveraineté de la Nouvelle-Zélande (Catalyst Cloud). Les noms de sous-domaines spécifiques des locataires ne sont pas énumérés dans cet article et sont intentionnellement masqués afin de réduire l'exposition de la surface d'attaque ; ils sont disponibles pour les évaluateurs légitimes sur simple demande adressée à l'auteur correspondant. Chaque configuration de type « village » actuellement opérationnelle authentifie ses membres et renvoie une réponse 302 / 403 aux requêtes de contenu non authentifiées — la signature opérationnelle d'un locataire actif. Une configuration de type « carpool » est en cours de développement sur l’infrastructure souveraine néo-zélandaise en tant que premier déploiement envisagé de fédération multi-instances ; le « carpool » isole les primitives de fédération et de backend administratif sans la surface d’exposition complète aux membres des autres types de « village », ce qui en fait l’illustration pédagogique la plus claire de la primitive de fédération. L’invitation aux communautés ou organisations intéressées par une participation au projet pilote se trouve au §7.4.

Type de village	Objectif (sélection parmi les applications possibles)
Whānau	Sites consacrés à la famille élargie maorie contenant des ressources généalogiques et d'h
Rūnanga	Sites des conseils iwi (tribaux) contenant des procès-verbaux, des décisions de comités et
Comité	Configurations d'organes délibératifs pour les fédérations sportives, les associations prof
Kāhui Māori	Sites de coordination multi-iwi où le partage s'effectue par le biais d'une fédération bilate
Gouvernance	Organismes institutionnels (conseils communautaires, conseils scolaires, conseils paroiss
Adhésion	Organismes affiliés au niveau national avec des sections locales — une association nation

La typologie développée ici s'étend au-delà des types de « villages » à une classe plus large de formes organisationnelles dont les intérêts structurels ne s'expriment pas individuellement mais collectivement. Les organes de codécision sectoriels dans les juridictions où la négociation collective est inscrite dans la Constitution — les comités d'entreprise en vertu de la Mitbestimmungsgesetz en Allemagne, les conseils représentatifs en vertu de l'Arbeitsverfassungsgesetz en Autriche, le conseil d'entreprise belge, les dispositifs scandinaves de samarbejdsudvalg — sont des formes organisées dont les intérêts en matière de souveraineté des données ne sont pas satisfaits par les seuls droits des personnes concernées. Les sociétés coopératives, où les droits des membres sont égaux et où les décisions sont régies par des assemblées de membres, partagent les mêmes exigences architecturales : une fédération bilatérale entre coopératives de différentes juridictions ; des registres souverains avec une portabilité pilotée par les membres ; une interface utilisateur de gouvernance des parties prenantes qui soutient la délibération collective. Les syndicats dans les juridictions où la représentation syndicale est institutionnalisée présentent la même structure. L'architecture n'impose aucune forme de gouvernance particulière ; elle expose les éléments fondamentaux dont toute forme de ce type a besoin.

D'autres types de villages dans la famille de modèles — famille (axée sur la généalogie), paroisse (communauté ecclésiale locale), entreprise (annuaire des membres et avis pour les petites associations de commerçants) et covoiturage (mise en relation de covoiturage, en cours de développement, support du premier déploiement envisagé de fédération multi-instances) — sont des instances concrètes de la même famille de modèles. L'ensemble n'est pas une liste figée ; la valeur du modèle réside précisément dans le fait que des types de villages supplémentaires peuvent être configurés sans modification de l'architecture.

11.1 Cohortes de couches linguistiques situées (référence anticipée à l'article B)

Chaque configuration de type de village est associée à une cohorte *de couche linguistique située* — un modèle linguistique par type de locataire formé sur le contenu propre au locataire selon une discipline de formation stricte. Les cohortes sont déployées pour les types de villages actuellement en production ; les cohortes désignées pour les types de villages supplémentaires attendent le premier locataire de chaque type avant leur mise en service, conformément à la discipline du projet contre la formation ambitieuse. Les résultats empiriques — notamment un ensemble documenté d'expériences de modification des poids montrant une dégradation uniforme, les quatre règles « sans X » d'hygiène des données d'entraînement, l' architecture d'inférence de secours sur CPU, et les résultats d'évaluation par cohorte — sont présentés séparément dans le résumé de l'article B.

Une barrière de pré-lancement est en place au niveau de la plateforme : la création de locataires est bloquée jusqu'à l'autorisation explicite de l'opérateur. La plateforme ne lance pas de locataires en silence ; la barrière garantit que chaque locataire opérationnel a franchi une étape d'autorisation qui est elle-même consignée dans un journal d'audit. Une barrière distincte de constitution souveraine applique un 403 strict aux locataires créés après le 01/05/2026 qui ne disposent pas des sections souveraines requises ; cette barrière est opérationnelle avec une immunité de suspension intégrée pour les locataires d'infrastructure de plateforme désignés.

---

12. Évaluation

Cette section rassemble les preuves de la mise en œuvre de l'architecture en un seul endroit. Trois registres et une étude de cas sont présentés : le registre de vérification des cas d'utilisation, le registre de consultation du cadre, l'instantané de déploiement et de vérification, et l'étude de cas sur la stabilité du hachage en mode d'hydratation datée du 22 avril 2026.

12.1 Configuration expérimentale

La plateforme fonctionne en production sur deux sites d'infrastructure : un déploiement sous souveraineté de l'UE sur OVH France (community.myfamilyhistory.digital et les sous-domaines de locataires associés sous mysovereignty.digital et myfamilyhistory.digital) et un déploiement sous souveraineté néo-zélandaise sur Catalyst Cloud (infrastructure village-nz desservant les sous-domaines de locataires de mysovereignty.digital). Les deux sites exécutent le même code à la même révision ; la parité des miroirs est maintenue entre les deux cibles de déploiement ainsi qu'un amont Forgejo auto-hébergé. La base de données est un MongoDB par site MongoDB avec des requêtes limitées au locataire, appliquées par un plugin Mongoose ; l'inférence d'exécution pour la couche de langage situé est hébergée sur un GPU souverain néo-zélandais (Catalyst A6000 pendant les heures de bureau, eGPU domestique en dehors des heures de bureau) avec basculement automatique.

12.2 Registre de vérification des cas d'utilisation Le

Le registre des cas d'utilisation démontre que chaque composant implémenté fonctionne comme prévu sur une base de données locale en production. Le registre couvre les composants architecturaux : la canonisation de la provenance ; le et ses modes de filtrage ; la mise en cache de vérification ; la signature de la chaîne de preuves, y compris les commandes UPDATE et DELETE en mode requête ; le chemin de tombstone de la file d'attente de gouvernance ; la publication DID ; le wrapper d'exportation y compris la superposition de visibilité ; les prérequis constitutionnels ; la surface de fédération ; la

migration des enregistrements souverains à travers les modèles de contenu générés par les locataires et la couverture des sous-documents intégrés ; le câblage au niveau du groupe, y compris la surface du fil de discussion ; les chemins d'exportation et d'ingestion canoniques DSR ; l'alignement des politiques des travailleurs ; l'adaptation des politiques WebSocket ; la mise à niveau des tombstones ; la compaction de la chaîne de preuves ; la surface de la porte d'accès ; les pages de visualisation par locataire. Le taux de réussite (PASS) du registre est à parité au moment de l'instantané ; l'ensemble de scripts est reproductible par un réviseur externe ayant accès au code source (l'annexe B résume les catégories).

12.3 Registre de consultation du cadre Le

Le registre de consultation du cadre couvre l'ensemble de l'architecture. Chaque enregistrement indique le service consulté, le verdict par condition et les métadonnées opérationnelles (nom de l'opération, durée, classe de résultat). L' ensemble des services actifs couvre les services Tractatus de base (BoundaryEnforcer, ContextPressureMonitor, MetacognitiveVerifier, PluralisticDeliberationOrchestrator, CrossReferenceValidator, InstructionPersistenceClassifier) ainsi qu'un ensemble plus large de services spécifiques à la prise de décision accumulés au fur et à mesure du développement de l'architecture (TractatusAuditRecorder, SovereigntyPrimacyEnforcer, PolicyCoherenceValidator, TenantIsolationValidator, AuditTrailVerifier, SchemaGuardian, PolicyDecisionOracle, TenantOwnerAuthority, PluralisticDeliberator, GovernanceOrchestrator). Le registre est enregistré de manière uniforme sur des bases de données de production locales ainsi que sous la souveraineté de l'UE et de la Nouvelle-Zélande — trois sites d'insertion par consultation — afin qu'aucune perte sur un seul hôte ne compromette la position d'audit. Un contrôle de santé programmé rend compte de l'actualité des consultations par service par rapport à des seuils ajustés pour un rythme de travail réaliste (4 heures à l'échelle du système, 24 heures par service) ; ces seuils ont remplacé les valeurs par défaut antérieures de 30 minutes qui généraient des alertes de perte de signal faussement positives à chaque brève interruption du développement actif.

12.4 Indicateurs de déploiement

État du déploiement au moment de l'instantané : les deux sites de production renvoient `/api/health` 200 ; les services du module du framework indiquent qu'ils sont opérationnels sur les deux sites ; verify-and-cache s'exécute chaque nuit sur les modèles de contenu générés par les locataires ; la surface de test de fumée de Catalyst (catalyst-operational) est validée avec une couverture complète ; ESLint s'exécute sans erreur sur les fichiers modifiés à chaque déploiement ; la parité des miroirs est maintenue entre `ovh`, `catalyst` et `forgejo`. Le verdict « FAIL » du test de fumée observé pendant les fenêtres de maintenance actives est un comportement attendu — le test de fumée interroge les points de terminaison de production qui servent le code HTML de maintenance pendant le verrouillage — et revient à « PASS » une fois la fenêtre de maintenance levée.

12.5 Observabilité du cache de vérification Le cache de vérification est alimenté sur l'ensemble des locataires opérationnels

Le cache de vérification est alimenté sur l'ensemble des locataires opérationnels des deux sites de production et couvre les onze types de contenu actuellement en usage. Les enregistrements sans hachage de provenance (un petit résidu d'enregistrements hérités antérieurs à la migration vers les enregistrements souverains) sont marqués `comme « non vérifiables »` plutôt que « `valides` ». La propriété architecturale est que le champ de vérification de chaque réponse GET de l'API affiche l'état du cache aux consommateurs ; les outils d'audit en aval peuvent déduire l'état de santé de la vérification de l'architecture en interrogeant l' interface de l'API, sans nécessiter d'accès à la base de données. La

contribution substantielle réside dans la discipline de l’observabilité, et non dans le nombre d’enregistrements.

12.6 Étude de cas : le bogue de stabilité du hachage en mode d'hydratation du 22/04/2026

L'événement empirique le plus instructif au cours du développement de l'architecture a été la découverte d'un bug de stabilité de hachage lors de la validation des cas d'utilisation de l'intégration du chemin de lecture du cache de vérification. Le sérialiseur de forme canonique itérait les propriétés énumérables d’un sous-document ORM — un modèle qui fonctionnait correctement pour les charges utiles d’objets simples mais qui révélait l’état interne de l’ORM pour les documents hydratés, produisant des hachages qui divergeaient selon les modes d’hydratation. Les hachages en temps de sauvegarde mettaient en cache une valeur ; les hachages en temps de lecture en calculaient une autre ; chaque enregistrement après le déploiement aurait affiché `une erreur « chain_hash_mismatch »`. La correction a consisté en une étape de normalisation d’une seule ligne. Le bogue avait passé la suite de tests unitaires sans encombre car les tests simulaient des entrées d’objets simples — le mode de défaillance nécessitait de véritables documents hydratés.

Il s’agit d’un exemple phare de la discipline opérationnelle : les tests prouvent que le câblage fonctionne dans les simulacres, mais la validation des cas d’utilisation par rapport à une base de données en production prouve que le câblage fonctionne dans la réalité. La discipline selon laquelle les tests prouvent ce que les simulacres révèlent, et la validation des cas d’utilisation met en évidence ce que les simulacres cachent, est inscrite dans la discipline opérationnelle du projet et explique pourquoi un ensemble de scripts de validation des cas d’utilisation coexiste avec la suite de tests unitaires. Après la correction, tous les enregistrements de production existants ont été remis en cache avec le sérialiseur de forme canonique corrigé ; aucun enregistrement n’a été perdu, aucune position d’audit n’a été compromise, et le bug est l’exemple canonique utilisé dans la formation à la discipline opérationnelle.

12.7 Interprétation

Les résultats de l'évaluation corroborent une affirmation spécifique : l'architecture est opérationnelle, observable et vérifiable au niveau de l'interface API sur plusieurs sites d'infrastructure souverains. La surface de vérification (registre des cas d'utilisation, registre de consultation du cadre, métriques de déploiement) est reproductible par tout réviseur ayant accès au code source ; l'étude de cas sur la stabilité des hachages démontre que la discipline opérationnelle détecte de véritables modes de défaillance que les tests simulés ne détectent pas. Ce que l'évaluation *ne* prétend*pas*, c'est que chaque menace mentionnée au §4 est complets défendue — l'architecture défend des invariants *nommés* avec des prédicats*nommés*; les menaces en dehors du modèle (attaques par chiffrement déniable ; compromission de la chaîne d'approvisionnement du cadre Tractatus ; compromission physique du matériel de la couche d'inférence) sont hors du champ d'application et sont suivies dans la discipline opérationnelle en tant que problématiques distinctes.

---

13. Approche open source

La posture open source se décline en deux volets.

Le **framework Tractatus** — le mécanisme de gouvernance en phase de développement — est public, open source sous licence Apache 2.0 et distribué sur `codeberg.org/mysovereignty/tractatus-framework` [1]. Son document de travail, ses modèles de code et ses métriques sont

reproductibles par un évaluateur externe ayant accès à une installation de type Claude-Code et à la bibliothèque de modèles du framework.

La **base de code de la plateforme** — l'application d'exécution — est publiée en open source module par module sous la licence publique de l'Union européenne version 1.2 (EUPL-1.2) [10]. Les fichiers source comportent des en-têtes EUPL-1.2 pour chaque fichier ; les fichiers les plus récemment modifiés de la plateforme (provenance, cache de vérification, attribution au niveau du groupe, hooks de suppression et de mise à jour en mode requête, exportation canonique DSR, services de fédération, composants d'interface utilisateur des parties prenantes, aides à la politique des travailleurs) portent cet en-tête. La licence au niveau du référentiel est en attente de la constitution d'une société de gouvernance en vertu de la législation néo-zélandaise, avec un conseil d'administration élu démocratiquement et un comité consultatif. Le conseil d'administration approuve les changements architecturaux qui ont une incidence sur la posture open source de la plateforme et les engagements des parties prenantes ; le comité consultatif fournit des conseils culturels et des avis des parties prenantes (conseils culturels maoris ; conseils des communautés linguistiques minoritaires ; conseils de la communauté FOSS). Le conseil d'administration n'a pas encore été constitué ; les en-têtes EUPL-1.2 par fichier constituent la préparation open source en cours, et non l'état final au niveau du référentiel.

La stratégie de publication module par module a été délibérément préférée à une publication globale du référentiel. La préoccupation sous-jacente concerne une catégorie de surfaces d'attaque des grands modèles linguistiques dans laquelle une publication globale du code source d'une plateforme à couplage interne expose du matériel dont le modèle de menace n'a pas été examiné au niveau des limites des modules — du code qui ne résiste qu'à certaines attaques parce qu'il n'a pas encore été lu par des modèles entraînés sur des corpus adversaires . Une publication minutieuse module par module permet d'examiner le modèle de menace de chaque module avant sa publication et limite la propagation du couplage interne vers des surfaces dépendantes de l'extérieur. Les modules publiés à ce jour — le plugin principal de registres souverains, le moteur d'héritage des politiques, le magasin de clés des locataires, le framework Tractatus, les composants du pipeline DSR — établissent la surface architecturale que les réviseurs externes peuvent utiliser ; les modules suivants suivent le même rythme de révision puis de publication.

Il existe un projet de licence « Village Model Licence » sous la forme d'un formulaire de licence personnalisé destiné à combiner les autorisations typiques des logiciels libres avec des clauses spécifiques de protection de la communauté (pas d'utilisation à des fins de surveillance des communautés ; pas d' utilisation qui enfreindrait les stipulations d'une communauté en matière de souveraineté des données ; pas d' utilisation qui contournerait la position déclarée d'un locataire vis-à-vis des principes CARE). Le projet est en attente d'un examen juridique formel ; en attendant le résultat de cet examen, la licence par fichier de la plateforme reste l'EUPL-1.2.

13.1 Discipline des fournisseurs

La plateforme n'utilise aucun cloud, SaaS ou infrastructure détenu par des entités américaines dans son chemin de requêtes de production. L'hébergement sous souveraineté européenne est assuré par OVH France ; l'hébergement sous souveraineté néo-zélandaise est assuré par Catalyst Cloud (avec Catalyst (NZ) Limited comme entité juridique) ; le basculement eGPU domestique pour l'inférence en dehors des heures de bureau s'effectue sur un processeur graphique non américain. L'hébergement du référentiel de code est divisé : une instance Forgejo auto-hébergée constitue le référentiel distant principal sous souveraineté européenne, avec des miroirs vers les référentiels nus d'OVH et de Catalyst. Le traitement des paiements utilise Airwallex (NZ) Limited — les réseaux de cartes américains ne sont utilisés qu'au cas par cas lorsque l'émetteur de la carte du payeur est basé aux

États-Unis, et uniquement pour cette transaction unique. Les outils de traduction utilisent DeepL (entité allemande, relevant de la juridiction du RGPD de l'UE). Cette discipline vis-à-vis des fournisseurs est imposée par une règle interne qui répertorie explicitement les fournisseurs autorisés et interdits ; toute dérogation nécessite une décision explicite au niveau du projet, et non une introduction tacite.

Aucune donnée biométrique n'est collectée par la plateforme. La vérification de l'identité des membres lors d'opérations à enjeux élevés est effectuée hors bande (présentation en personne au sein de la communauté ; présentation par vidéo ; vérification par voie papier) ou via la clé de signature d'identifiant décentralisé contrôlée par le membre, jamais via la capture biométrique. Le raisonnement est structurel et converge selon quatre axes : les données biométriques sont irrévocables, de sorte qu'une fuite ne peut être corrigée par rotation ; les données biométriques présentent trois voies d'exposition structurelles à la juridiction américaine (capture directe du côté américain aux frontières et lors des entretiens de visa ; hébergement dans le cloud américain soumis à l' à la contrainte du CLOUD Act quelle que soit la nationalité de la personne concernée ; les futurs accords de partenariat renforcé pour la sécurité aux frontières envisageant un accès direct aux bases de données biométriques des pays partenaires) ; les données biométriques et ADN maories bénéficient d'une protection spécifique au titre du Te Tiriti / WAI 262 / WAI 2522 qui s'applique dès lors que ces données sont collectées par la plateforme, et l'exposition de ces données par la Couronne à un régime juridictionnel étranger met à l'épreuve la protection des taonga prévue par l'article 2 d'une manière que la plateforme ne doit pas exclure ; et les interfaces de programmation d'applications biométriques les plus ergonomiques sont exploitées par des entreprises dont le siège social est aux États-Unis et dont l'utilisation violerait de toute façon la règle d'interdiction des fournisseurs de la plateforme. Le Le refus de collecter des données biométriques soustrait architecturalement la plateforme à l'ensemble de cette surface de risque — l' opérateur ne peut être contraint de divulguer ce qui n'a jamais été collecté. Les membres qui souhaitent utiliser le déverrouillage biométrique local sur leur appareil pour accéder à leur propre coffre-fort d'identifiants peuvent le faire sur leur propre matériel ; les données biométriques ne franchissent jamais les limites de la plateforme, et celle-ci n'interfère pas avec ce schéma. La surface d'accès propre à la plateforme — y compris la passerelle d'accès souveraine fournie (§15), dont l'activation par locataire est gérée par l'opérateur — utilise des phrases de passe textuelles (mots aléatoires / style liste de mots de l'EFF ; à haute entropie et renouvelables) ainsi qu'une détection des bots par preuve de travail auto-hébergée.

13.2 Le périmètre de propriété intellectuelle

La stratégie de publication distingue la *structure architecturale* (publisable sous forme de contenu papier ; publiée sous forme de modules open source) des *spécificités opérationnelles* (retenues pour des raisons de périmètre IP). Sont retenues : les conditions spécifiques de consultation du cadre Tractatus par service (le catalogue constitue la contribution du cadre) ; contenu du vocabulaire par type de produit au-delà de la famille de modèles de haut niveau ; spécificités de configuration par locataire ; détails spécifiques de l'ensemble de champs du manifeste de fédération au-delà de la structure architecturale de l'annexe C. Publié : les primitives architecturales dans le document ; le modèle de menace et les prédicats testables ; les structures de schémas de haut niveau ; les limitations et les modes de défaillance (§15) ; les modules sources selon le plan de publication module par module.

---

14. La contribution architecturale

L'architecture est une réponse à une condition structurelle, et non un produit concurrent. Le modèle par défaut de la plateforme communautaire — détenue par les États-Unis, captant

l'attention, dont les conditions d'utilisation peuvent être révisées à volonté — est un choix architectural particulier concernant le lieu où réside la souveraineté des données. Un choix architectural ne peut trouver de réponse que dans une alternative architecturale, et non dans des révisions des conditions d'utilisation ou des ajouts de fonctionnalités aux plateformes existantes.

Quatre propriétés du travail ont une incidence sur ce point.

Le travail est **opérationnel**. L'architecture n'est pas une spécification en attente de mise en œuvre. Elle fonctionne, à travers de multiples configurations de type « village », sur des infrastructures relevant de la souveraineté de l'UE et de la Nouvelle-Zélande. Un évaluateur peut vérifier l'état opérationnel via l'interface API et vérifier chaque décision architecturale via le registre de consultation du cadre persistant. Le registre de vérification des cas d'utilisation couvre l'interface architecturale mise en œuvre à parité. La contribution substantielle réside dans la discipline de l'enregistrement — le fait que l'architecture produise des artefacts d'audit observables de l'extérieur sans avoir à se fier à la parole de l'opérateur.

Le travail est **structurellement portable**. L'architecture ne fait pas spécifiquement référence aux communautés maories, au te reo maori ou au Te Tiriti. Le même champ `metadata.origin.collective_id` qui permet à une communauté maorie d'attribuer un enregistrement à son rūnanga permet à une une communauté galloise d'attribuer un enregistrement à sa paroisse, une communauté sami à sa siida, une communauté sorabe à son village. Le modèle de couche linguistique située est tout aussi portable : une couche en langue galloise entraînée sur du matériel en langue galloise sous l'autorité de la communauté galloise répond aux requêtes en gallois avec la même posture architecturale que la couche en langue maorie répond aux requêtes en maori. L'architecture est un substrat, pas un produit.

Le travail est **compatible avec la fédération**. L'infrastructure de fédération bilatérale est fournie de bout en bout avec une matrice de tests négatifs exhaustive couvrant la portée, le blocage d'écriture, l'audit, la discipline de citation, la mise en cache, les cas limites, l'autorisation et la séparation des espaces de noms de phase 3. Les liens de fédération actifs entre des déploiements de locataires indépendants sont en attente du premier déploiement multi-instances ; la propriété architecturale — selon laquelle deux communautés peuvent convenir, selon des termes qu'elles spécifient, d'une interaction délimitée spécifique, et uniquement celle-ci — est exactement ce que les trois articles du Te Tiriti impliquent pour l'infrastructure numérique, et ce dont les communautés de langues minoritaires en Europe ont besoin lorsque leur travail intercommunautaire chevauche des juridictions légales.

Le travail **respecte la portabilité**. Un membre est une personne concernée de premier ordre. Il peut exporter l'intégralité de son ensemble de données sous une forme cryptographiquement vérifiable et le migrer vers n'importe quel autre tenant fonctionnant selon le même modèle architectural. L'exportation est symétrique au droit d'accès prévu à l'article 15 du RGPD ; la migration est symétrique à l'engagement architectural selon lequel la sortie est une opération de premier ordre. Un modèle communautaire où la sortie est difficile est un jardin fermé, quel que soit le langage marketing utilisé ; un modèle communautaire où la sortie est architecturale est ce que le travail présenté ici rend possible.

L'argument de fond de l'architecture est qu'une plateforme à l'échelle d'une communauté peut être construite de telle sorte que ses propriétés de souveraineté résident au niveau des enregistrements et de l'infrastructure des locataires, et non à la discrétion de l'opérateur. Le modèle par défaut repose sur une souveraineté accordée par l'opérateur et révocable par celui-ci ; une alternative architecturale — la souveraineté en tant que propriété des enregistrements et de l'infrastructure des locataires — refuse cette condition par construction. Le travail présenté ici est une preuve concrète qu'une telle alternative peut être mise en place par une petite équipe en Nouvelle-Zélande, avec un budget modeste, et fonctionner en production pour de véritables communautés, même si l'environnement

réglementaire continue de s’orienter vers une ingérence des juridictions étrangères (le Partenariat pour la sécurité renforcée des frontières en étant l’exemple concret en Nouvelle-Zélande).

---

15. Limites et modes de défaillance Plusieurs éléments entrent dans le champ d’application des affirmations de cet article mais ne sont pas déployés

Plusieurs éléments entrent dans le champ d’application des affirmations de cet article mais ne sont pas déployés au moment de la rédaction de ce projet :

- **Trafic de fédération de covoiturage en direct.** L’infrastructure de fédération bilatérale est livrée de bout en bout avec une surface de vérification substantielle, mais aucune fédération en direct entre des déploiements de locataires indépendants n’a été activée. Le déploiement de fédération de covoiturage, envisagé comme la première illustration multi-instances, est mené au rythme de l’opérateur.
- **Cohortes de couche de langage situé de niveau 2.** Les cohortes désignées pour des types de villages supplémentaires sont mises en attente conformément à la discipline du projet en matière de formation ambitieuse : une cohorte n'est pas mise en service tant que le premier locataire de ce type n'est pas déployé.
- **Publication open source complète au niveau du référentiel.** Les en-têtes EUPL-1.2 par fichier de la plateforme sont en place ; la publication module par module est en cours ; la licence au niveau du référentiel est en attente d’ approbation par le Conseil d’administration, et le Conseil d’administration lui-même est en attente de constitution en société en vertu de la loi néo-zélandaise.
- **Publication de la déclaration de conformité Tiriti v0.2.** Une révision v0.2 existe sur la base du meilleur jugement de l'agent délégué par l'opérateur ; la publication sous ce nom nécessite le consentement explicite du Dr Taiuru.
- **Examen juridique formel de la licence Village Model.** Le projet existe ; l'examen juridique formel est en attente ; en attendant son résultat, la licence par fichier de la plateforme reste l'EUPL-1.2.
- **Réconciliation d'identité des locataires récepteurs et intégration automatique.** Le chemin d'ingestion actuel de la migration DSR refuse l'intégration automatique par défaut ; l'intégration automatique via un DID inter-locataires constitue une surface de sécurité qui justifie sa propre phase de conception.
- **Passerelle d'accès souveraine (phrase de passe + preuve de travail souveraine détection des bots + codes de récupération papier) — livrée, déploiement par locataire au rythme de l'opérateur.** L'authentification de base de la plateforme repose sur des cookies httpOnly ainsi que sur l'isolation du contexte du locataire appliquée au niveau de la couche de requêtes de la base de données. Le composant de passerelle d'accès est livré de bout en bout sous la forme d'un middleware de pipeline de requêtes global (`accessGate`) avec un `AccessGateConfig` par locataire (hachage de la phrase de passe, historique de rotation, nombre de codes de récupération), dix points de terminaison REST (`/api/access-gate/{status, pow/{challenge,verify}, passphrase/verify, recovery/use, admin/{enable,disable,rotate,status,recovery-codes/pdf}}`), une paire de défis/vérifications de preuve de travail auto-hébergée (pas de service tiers de détection de bots), et des codes de récupération imprimables sur papier générés sous forme de PDF à la demande de l'opérateur (pas de SMS, pas d'e-mail, pas de canal hors bande acheminé via l'infrastructure américaine). Le composant est désactivé par défaut sur chaque tenant ; le déploiement par tenant — émission de mot de passe, distribution des codes de récupération, intégration des membres à la passerelle — est mené au rythme de l'opérateur et se déroule tenant

par tenant sous contrôle documenté. L'engagement architectural en faveur d'une authentification par SMS uniquement et sans données biométriques, tel qu'énoncé dans la discipline des fournisseurs du §13.1 et l'invariant I9 du §4, est permanent et est appliqué aujourd'hui par la politique existante de la plateforme consistant à ne collecter aucune donnée biométrique, indépendamment de l'état de déploiement de la passerelle par locataire. Les rejets architecturaux explicites dans la conception de la passerelle — authentification biométrique, authentification à deux facteurs par SMS, liens magiques par e-mail via des fournisseurs hébergés aux États-Unis, OTP push contrôlé par les États-Unis, services de détection de bots contrôlés par les États-Unis, biométrie comportementale — sont documentés dans le plan d'enregistrement de la passerelle d'accès avec le raisonnement qui a motivé chaque rejet, de sorte que la surface de choix est permanente plutôt que le fruit d'une omission. Ce qui reste du ressort de l'opérateur, c'est la décision d'activation par locataire, et non l' existence du composant.

- **Personnalité juridique des agents IA — question ouverte, traitée dans le document B.** Le Dr Taiuru (2026) [25a] pose, à titre d'enquête ouverte, la question de savoir si et dans quelles conditions la personnalité juridique pourrait être étendue aux agents IA constitués par le savoir maori, renvoyant expressément la décision à un travail collectif entre les développeurs d'IA, les agences gouvernementales et les communautés maories. L'article B, qui l'accompagne, rend compte de la discipline de formation par cohortes de couches linguistiques situées sur laquelle s'appuierait tout futur travail de partenariat par cohortes ; le présent article ne préjuge pas ni ne préjuge de ce travail.

Les menaces ne relevant pas du modèle §4 sont suivies séparément dans le cadre de la discipline opérationnelle : attaques par cryptage déniable contre le magasin de clés ; compromission de la chaîne d'approvisionnement du cadre Tractatus ou de ses dépendances ; compromission physique du matériel de la couche d'inférence ; obsolescence des primitives cryptographiques hors de portée du wrapper d'agilité algorithmique. Aucune de ces menaces n'est abordée dans cet article ; toutes constituent de réelles préoccupations au niveau de la mise en œuvre et méritent une analyse spécifique.

Deux limitations structurelles sont inhérentes plutôt que liées à la mise en œuvre. L'architecture préserve la souveraineté de la communauté sur les données ; elle ne préserve pas en soi la souveraineté de la communauté sur *la cognition*. Une communauté utilisant la couche de langage situé pour servir d'intermédiaire aux requêtes de ses membres utilise toujours un modèle de langage ; le corpus d'entraînement du modèle, la discipline d'entraînement et le comportement d'exécution font partie de la surface de l'architecture, et ne sont pas distincts de celle-ci. L'article B documentera la discipline d'entraînement empirique qui rend la couche de langage situé fiable pour une utilisation par la communauté ; ses résultats limitent les conclusions qu'un lecteur peut tirer de cet article seul. L'autre limitation structurelle est que la défense de l'architecture contre l'adversaire A1 de la section 4 (opérateur hôte contraint par la juridiction) dépend en fin de compte du fait que le locataire exploite sa propre infrastructure ou s'associe à un hôte relevant d'une juridiction souveraine : l'architecture ne peut pas créer de souveraineté là où la juridiction de l'hôte ne la prend pas en charge, mais elle peut préserver la souveraineté pour les locataires dont les hôtes relèvent eux-mêmes d'une juridiction souveraine.

---

16. Conclusion

L'architecture décrite ici est mise en œuvre et fonctionne sur des infrastructures relevant de la souveraineté de l'UE et de la Nouvelle-Zélande. Ses éléments fondamentaux sont opérationnels : l'isolation des locataires en tant qu'élément fondamental ; des métadonnées

uniformes pour les enregistrements souverains dans tous les modèles de contenu générés par les locataires ; la provenance cryptographique avec flexibilité algorithmique ; l'héritage des politiques avec contrôle des politiques effectives à la limite de lecture ; signature de la chaîne de preuves sur les créations, mises à jour et suppressions (en mode document et en mode requête) ; mise en cache de vérification apparue au moment de la lecture ; magasin de clés par locataire avec finalité de suppression cryptographique ; publication d'identifiants décentralisés ; file d'attente de gouvernance avec piste de décision signée ; wrapper d'exportation avec superposition de visibilité non administrative et journalisation d'audit symétrique ; fédération bilatérale avec manifeste signé ; portabilité souveraine pilotée par les membres avec ingestion par le locataire destinataire symétrique selon l'article 15 ; couche de langage située par type de locataire ; interface utilisateur de gouvernance des parties prenantes avec interface de révision en lecture seule (phases 1 à 5) plus l'interface de dialogue participatif supervisé de la phase 6 livrée (file d'attente éditoriale validée par l'opérateur, porte de rédaction et de publication, pas de publication automatique), généralisée à tous les types de produits de la plateforme dans la phase 7 ; alignement des politiques des travailleurs et des WebSockets ; primitive de compactage de la chaîne de preuves ; primitive de mise à niveau des tombstones ; et la passerelle d'accès souveraine livrée (phrase de passe textuelle + détection des bots par preuve de travail auto-hébergée + codes de récupération sur papier ; déploiement par locataire au rythme de l'opérateur).

Le registre de consultation du cadre couvre l'ensemble de l'architecture (chaque consultation étant enregistrée de manière uniforme dans des bases de données de production locales ainsi que souveraines de l’UE et de la Nouvelle-Zélande) ; le registre de vérification des cas d’utilisation couvre les composants architecturaux implémentés à parité ; l’infrastructure de fédération bilatérale est livrée de bout en bout avec une matrice de tests négatifs exhaustive (un sous-ensemble étant en outre parcouru par un validateur multi-locataires en direct), avec des liens de fédération en direct entre des locataires indépendants en attente de la première activation de covoiturage multi-instances ; les cohortes de couches linguistiques situées par type de village sont opérationnelles ; les cohortes désignées pour des types de villages supplémentaires attendent le premier locataire de chaque type avant leur mise en service, conformément à la discipline du projet en matière de formation ambitieuse.

L'article d'accompagnement (Article B — Couches linguistiques situées pour les communautés de langues minoritaires et autochtones, synopsis de l’article empirique d’accompagnement, publié) décrit le modèle architectural des cohortes de couches linguistiques situées : des IA par type de communauté entraînées sur les propres enregistrements de cette communauté, les principes de fonctionnement que le projet suit lors de leur entraînement et de leur exécution, les déploiements de niveau 1 en cours aujourd’hui, et l’architecture d’inférence de secours sur CPU qui maintient le chemin d’exécution entièrement en dehors de l’infrastructure contrôlée par les États-Unis. L'article empirique complet — comprenant une évaluation par cohorte, des ablations de modification de poids, une analyse de la littérature comparative et un examen approfondi de l'ensemble des travaux du Dr Taiuru sur la gouvernance de l'IA maorie — à la fois le cadre Kaupapa Māori AI [25b] (les principes normatifs fondés sur le Te Tiriti pour le consentement en matière d’IA, la souveraineté des données et la responsabilité tout au long de la chaîne) et l’étude plus récente [25a] (la question ouverte de la personnalité juridique des agents IA constitués à partir des connaissances maories, que le Dr Taiuru renvoie expressément au travail collectif entre les développeurs d’IA, les agences gouvernementales et les communautés maories) — est mise en attente jusqu’à ce que des données de formation vérifiées soient disponibles. L'article complet est le lieu où les deux registres que le Dr Taiuru distingue — le devoir de gouvernance normatif et la question interrogative de la personnalité juridique — auront une incidence directe sur la discipline de cohorte faisant l'objet du rapport. L'article complet s'appuiera sur le test Tikanga de Mead (tapu, mauri, take-utu-ea, whanaungatanga) comme cadre d'évaluation sur lequel s'appuierait tout futur travail de partenariat par cohorte ; il ne préjuge pas non plus de ce travail de partenariat, mais rendra compte de la discipline de

formation de la cohorte avec le niveau de détail empirique qu'un tel travail de partenariat exigerait.

Cet article se présente comme un exemple concret de la manière dont la souveraineté architecturale peut répondre au Te Tiriti, à la personnalité juridique de l'IA (Dr Taiuru 2026) et aux pressions juridictionnelles de la classe EBSP sur le budget d'une petite équipe. L'architecture est la contribution ; le déploiement, l'engagement de l'auteur correspondant à faire fonctionner l'architecture dans le cadre des contraintes contre lesquelles elle se défend, en est la preuve. Les commentaires et corrections adressés à l'auteur correspondant sont les bienvenus.

Remerciements

L'auteur remercie Leslie Stroh pour son mentorat philosophique fondamental sur la pensée pluraliste et la question du bien dans l'intelligence artificielle. L'engagement en faveur de la délibération pluraliste qui imprègne l'architecture de gouvernance de la plateforme — ainsi que la conviction plus large qu'un substrat d'IA digne d'être construit doit répondre à une notion substantielle du bien, et non à une notion procédurale — doit sa forme initiale à ces conversations.

L'auteur remercie également le Dr Karaitiana Taiuru pour son examen de la sécurité culturelle de la Déclaration de conformité au Tiriti v0.1 ; la citation nominative des révisions ultérieures est subordonnée à son consentement direct et n'est pas mentionnée ici. Les relecteurs des premières ébauches du rapport de mise en œuvre précédent (v0.4) ont fourni un cadre qui a été repris dans cet article ; leurs contributions sont remerciées avec gratitude.

Annexe A — Reproductibilité

Un évaluateur souhaitant examiner la surface de reproductibilité de l’architecture peut le faire aux niveaux suivants.

Le framework Tractatus est le composant entièrement public, distribué sur `codeberg.org/mysovereignty/framework` sous licence Apache 2.0. Son document de travail consigne les conclusions d’observation du framework et les modèles architecturaux qu’il codifie. Un évaluateur ayant accès à une installation de classe Claude-Code peut reproduire la bibliothèque de modèles du framework et reproduire l’enregistrement des consultations sur une base de données locale.

Les modules publiés de la plateforme — sous licence EUPL-1.2 dans le cadre de la publication module par module — définissent l’interface architecturale que les évaluateurs externes peuvent utiliser. À ce jour, les modules couvrent le plugin central sovereign-record, le moteur d’héritage des politiques, le magasin de clés des locataires, les composants du pipeline DSR et l’infrastructure d’enregistrement des consultations du framework.

Les composants architecturaux sont décrits dans cet article au niveau de leurs interactions et de leurs contrats. Les chemins d’accès spécifiques (noms de fichiers dans l’arborescence source de la plateforme) ne sont intentionnellement pas énumérés ; la reproductibilité au niveau des fichiers et des lignes est préservée via les modules publiés, tandis que les spécificités opérationnelles (pipeline de déploiement, portes de maintenance, optimisation des hooks) sont considérées comme des détails d’ingénierie plutôt que comme une contribution à la recherche.

Les scripts de vérification des cas d'utilisation suivent une convention de nommage`validate-use-cases-*`; les scripts d'enregistrement des consultations du cadre suivent une convention

de nommage`record-*-consultation`. Chaque script de consultation produit une insertion idempotente d'enregistrements dans les bases de données de production locales ainsi que dans celles relevant de la souveraineté de l'UE et de la Nouvelle-Zélande, avec un identifiant par révision .

La reproduction du modèle de consultation du cadre, du côté du cadre Tractatus, est documentée dans [1].

Annexe B — Instantané du registre de vérification des cas d'utilisation

Un instantané actuel du registre des cas d'utilisation couvre plus de 45 scripts de validation distincts. Chaque script vérifie une propriété nommée d'un composant architectural par rapport à une base de données locale en production ; les scripts sont exécutables indépendamment et de manière agrégée. Les catégories ci-dessous résument l'ensemble des scripts ; le nombre de scénarios par script et les résultats PASS/FAIL sont inclus dans les artefacts internes du projet et sont reproductibles par un réviseur externe ayant accès au code source :

- Canonisation de la provenance et stabilité à travers les modes d'hydratation
- Moteur d'héritage des politiques : résolution de base ; câblage « gate-and-filter » ; filtrage « origin-only » ; filtrage au niveau du groupe ; mode strict « unknown-scope »
- Mise en cache de vérification : service d'ingestion ; hook post-enregistrement + balayage planifié ; intégration du chemin de lecture ; hook post-enregistrement du chemin de mise à jour
- Magasin de clés des locataires : opérations du cycle de vie
- Signature de la chaîne de preuves : consommateur CREATE ; mode document UPDATE/DELETE ; mode requête DELETE ; mode requête UPDATE ; tombstone de la file d'attente de gouvernance
- Publication DID : documents de locataire + de membre
- Câblage de la file d'attente de gouvernance
- Conteneur d'exportation : comportement par mode ; intégration ; journalisation d'audit du chemin de réussite ; superposition de visibilité pour les modes de hachage et d'agrégation
- Prérequis constitutionnels et prise en charge multilingue
- Migration des enregistrements souverains : à travers les modèles de niveau supérieur générés par le locataire ; couverture des sous-documents intégrés (NewsPost, Resource, EventMenu, Edition) ; phases 1+2 des sous-documents
- Câblage au niveau du groupe et attribution inter-formulaires
- Exportation canonique DSR : assemblage de paquets ; signature de manifeste ; intégrité du drapeau de troncature ; ingestion de bout en bout par le locataire destinataire
- Passerelle de politique des workers : tests unitaires d'aide ; intégration par worker (EmailProcessor, DocumentScanner)
- Adaptateur de politique WebSocket
- Mise à niveau des tombstones
- Compactage de la chaîne de preuves
- Surface de fédération : matrice de tests négatifs sur douze catégories, avec un sous-ensemble parcouru par un validateur multi-locataires en production

Annexe C — Référence du schéma du manifeste de fédération

Un enregistrement d’accord de fédération contient le manifeste bilatéral au niveau des composants architecturaux. Le schéma nomme : l'identifiant de l'accord ; chaque partie (identifiant du locataire, identifiant décentralisé du locataire, signature, horodatage de la signature) ; l'objectif délimité (une énumération : mise en relation de covoiturage ; annonce d'événement partagé ; délibération conjointe ; co-gestion du kaupapa ; référence

de nommage interdomaines ; et autres) ; la forme du flux de données par direction (champs exposés ; transformation appliquée ; conservation du côté récepteur) ; la règle de résolution des politiques (quelle constitution s'applique ; comment les conflits de politiques sont résolus, y compris un tableau explicite par champ) ; la procédure de révocation (unilatérale par l'une ou l'autre partie ; propagation immédiate ; les deux parties conservent une copie signée à des fins d'audit) ; et les identifiants de conservation d'audit (enregistrements de journaux de requêtes inter-locataires de chaque côté). Le manifeste lui-même contient le bloc de métadonnées standard des enregistrements souverains (origine, politique, chiffrement, chaîne de preuve, cache de vérification) ; une fédération ne s'active pas sans les signatures vérifiées des deux parties par rapport à leurs documents DID respectifs.

Les détails spécifiques de l'ensemble de champs de mise en œuvre au-delà de cette structure architecturale sont conservés conformément à la posture de périmètre IP (§13.2). Les évaluateurs ayant besoin des spécifications complètes du schéma pour l'évaluation de la compatibilité peuvent les obtenir en adressant une demande directe à l'auteur correspondant dans le respect de la confidentialité appropriée.

Références

[1] Stroh, J. G. (2026). *Tractatus Framework — Architectural Patterns for AI Development Governance, Working Paper v0.2.* `codeberg.org/mysovereignty/tractatus-framework`. Apache 2.0.

[2] Stroh, J. G. (2026). *Sovereign AI Governance at Community Scale — An EU Policy Brief, v0.1.* My Digital Sovereignty Limited. DOI: 10.5281/zenodo.19635598. CC BY 4.0.

[3] Stroh, J. G. (2026). *Équité distributive par la structure — Un exemple concret à l'échelle communautaire de la pérennité des valeurs, v1.0.* My Digital Sovereignty Limited. DOI : 10.5281/zenodo.19600614. CC BY 4.0.

[4] Carroll, S. R., Garba, I., Figueroa-Rodríguez, O. L., Holbrook, J., Lovett, R., Materechera, S., Parsons, M., Raseroka, K., Rodriguez-Lonebear, D., Rowe, R., Sara, R., Walker, J. D., Anderson, J., & Hudson, M. (2020). Les principes CARE pour la gouvernance des données autochtones . *Data Science Journal*, 19(1), 43. doi.org/10.5334/dsj-2020-043.

[5] Tribunal de Waitangi. (2011). *Ko Aotearoa Tēnei : Rapport sur les réclamations concernant la législation et les politiques néo-zélandaises affectant la culture et l' identité maories (WAI 262).* Legislation Direct, Wellington.

[6] Commission européenne. (2024). *Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées en matière d'intelligence artificielle (loi sur l'intelligence artificielle).*

[7] Commission européenne. (2024). *Règlement (UE) 2024/1083 du Parlement européen et du Conseil du 11 avril 2024 établissant un cadre commun pour les services de médias dans le marché intérieur (loi européenne sur la liberté des médias).*

[8] Parlement européen et Conseil. (2016). *Règlement (UE) 2016/679 (Règlement général sur la protection des données),* articles 9, 15, 16, 17, 18, 20, 21.

[9] Congrès des États-Unis. (2018). *Loi clarifiant l'utilisation légale des données à l'étranger (CLOUD Act),* Pub. L. n° 115–141, Div. V (23 mars 2018).

[10] Licence publique de l'Union européenne v1.2 (EUPL-1.2). https://joinup.ec.europa.eu/collection/eupl. Approuvée par la Commission européenne, 2017.

[11] World Wide Web Consortium. (2022). *Identifiants décentralisés (DID) v1.0 — Architecture de base, modèle de données et représentations.* Recommandation du W3C.

[12] Stroh, J. G. (2026). *Architecture de registres souverains pour les plateformes à l'échelle communautaire — Rapport de mise en œuvre de la phase 1, v0.4.* My Digital Sovereignty Limited (NZ). Version préliminaire de ce document ; conservée comme archive historique de l'état de l'architecture de la phase 1.

[13] Radio New Zealand / 1News. (février 2026). *Le MFAT confirme les discussions sur le Partenariat renforcé pour la sécurité aux frontières avec les États-Unis.* Déclaration officielle du ministère des Affaires étrangères et du Commerce.

[13a] Tribunal de Waitangi. *Enquête WAI 2522.* Deux rapports finaux pertinents pour le présent document : (i) *Rapport sur l'Accord de partenariat transpacifique* (2016) ; (ii) *Rapport sur l'Accord global et progressif de partenariat transpacifique* (2021). Un troisième rapport relevant de la même enquête WAI 2522 — *Rapport sur l'examen par la Couronne du régime des droits d'obtenteur* (2020) — est connexe mais n'est pas cité ici. Tous sont disponibles sur waitangitribunal.govt.nz.

[14] Centrist.nz. (2026). *Accord de sécurité frontalière entre la Nouvelle-Zélande et les États-Unis : état d'avancement des négociations.* Consulté via la couverture par centrist.nz des discussions sur l'EBSP.

[15] Oceanic Press. (2026). *Discussions sur l'EBSP : des responsables confirment que le champ d'application et les exigences font l'objet de négociations.*

[16] Privacy Foundation New Zealand. (2026). *Prise de position sur le partage de données biométriques avec les États-Unis dans le cadre du Partenariat renforcé pour la sécurité aux frontières.* Communiqué de presse de la Privacy Foundation NZ.

[17] Biometric Update. (2026). *La Nouvelle-Zélande envisage l'accès des États-Unis aux informations biométriques et d'identité des citoyens dans le cadre des discussions sur l'EBSP .*

[18] Gunasekara, G. (2026). *Analyse du Partenariat renforcé pour la sécurité aux frontières et des dispositions relatives à l'accès direct à la base de données du DHS.* Commentaire juridique de l'Université d'Auckland.

[19] Cochrane, T. (2024). *La Nouvelle-Zélande devrait-elle rechercher un accord exécutif de type CLOUD Act ? Implications pour la vie privée numérique.* Recherche financée par le Commissaire à la protection de la vie privée.

[20] Snell, J., & Prodromou, E. (2018). *ActivityPub.* Recommandation du W3C, 23 janvier 2018. https://www.w3.org/TR/activitypub/

[21] Bluesky Public Benefit Corporation. (2024). *Spécification du protocole AT.* https://atproto.com . Portabilité des comptes + résolution des identifiants décentralisés (basée sur les DID).

[22] Mansour, E., Sambra, A. V., Hawke, S., Zereba, M., Capadisli, S., Ghanem, A., Aboulnaga, A., & Berners-Lee, T. (2016). *Une démonstration de la plateforme Solid pour les applications Web sociales.* Companion de la 25e Conférence internationale sur le World Wide Web. Plus Travaux de spécification en cours du groupe communautaire W3C Solid sur https://solidproject.org.

[23] McMahan, H. B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017). *Apprentissage efficace en termes de communication des réseaux profonds à partir de données décentralisées.* Dans *Artificial Intelligence and Statistics (AISTATS)*. L'article original sur l'apprentissage fédéré .

[24] Kairouz, P., et al. (2021). *Advances and Open Problems in Federated Learning. Foundations and Trends in Machine Learning*, 14(1-2), 1-210. Étude exhaustive des choix architecturaux en matière d'apprentissage fédéré et des problèmes en suspens.

[25] Walter, M., & Suina, M. (2019). *Données autochtones, méthodologies autochtones et souveraineté des données autochtones. International Journal of Social Research Methodology*, 22(3), 233-243.

[25a] Taiuru, K. (3 mai 2026). *Agents IA et personnalité juridique en Nouvelle-Zélande.* `taiuru.co.nz/ai-agents-and-legal-personhood-in-new-zealand/.` Consulté le 03/05/2026. Article d'opinion personnelle (accompagné d'une mention explicite de l'auteur précisant qu'il s'exprime à titre personnel). Pose la question de la personnalité juridique comme une interrogation ouverte, renvoyant la décision à un travail collectif entre les développeurs d'IA, les agences gouvernementales et les communautés maories.

[25b] Taiuru, K. (6 mars 2026). *Cadre Kaupapa Māori pour l'IA — He Tangata, He Karetao, He Ātārangi.* `taiuru.co.nz/kaupapa-maori-ai-framework/.` Consulté le 04/05/2026. Cadre d'IA des peuples autochtones fondé sur le Te Tiriti o Waitangi et la Déclaration des Nations Unies sur les droits des peuples autochtones (UNDRIP) ; énonce comme pratiques obligatoires le consentement maori et la souveraineté des données sur le matériel de formation, ainsi que la responsabilité tout au long de la chaîne entre développeurs, opérateurs et déployeurs.

[22b] Symmetry Systems. (2024). *Sécuriser votre pile de données souveraines et d'IA .* Analyse sectorielle de l'architecture de l'IA souveraine.

[23b] Merit Data Tech. *IA sans sortie : conception de modèles linguistiques situés sur site pour une souveraineté des données vérifiable.* Analyse sectorielle.

[24b] Enterprise DB. *IA souveraine : garantir la souveraineté des données et de l'IA dans les entreprises.*

[26] Wachter, S., Mittelstadt, B., & Floridi, L. (2017). *Pourquoi le droit à une explication de la prise de décision automatisée n'existe pas dans le règlement général sur la protection des données.* International Data Privacy Law, 7(2), 76–99. DOI: 10.1093/idpl/ipx005. Cité au §3.5.

[27] Edwards, L., & Veale, M. (2017). *Esclave de l'algorithme ? Pourquoi un « droit à une explication » n'est probablement pas la solution que vous recherchez.* Duke Law & Technology Review, 16(1), 18–84. Disponible à l'adresse scholarship.law.duke.edu/dltr/vol16/iss1/2. Cité au §3.5.

[28] Te Mana Raraunga (Réseau maori pour la souveraineté des données). (2018, octobre). *Principes de la souveraineté des données maories.* Extrait de temanararaunga.maori.nz/principles-of-maori-data-sovereignty. Cité dans §3.6.

[29] Carroll, S. R., Rodriguez-Lonebear, D., & Martinez, A. (2019). *Gouvernance des données autochtones : stratégies des nations autochtones des États-Unis.* Data Science Journal, 18, 31. DOI : 10.5334/dsj-2019-031. Cité dans §3.6.

[30] Hudson, M., Anderson, T., Dewes, T. K., Temara, P., Whaanga, H., & Roa, T. (2017). *« He Matapihi ki te Mana Raraunga » — Conceptualiser le Big Data à travers le prisme maori.* Disponible via Research Commons, Université de Waikato. Cité au §3.6.

[31] Raman, A., Joglekar, S., De Cristofaro, E., Sastry, N., & Tyson, G. (2019). *Les défis du Web décentralisé : le cas de Mastodon.* Dans les Actes de la Conférence sur la mesure de l'Internet 2019 (IMC '19), Amsterdam, octobre 2019. Caractérisation empirique du graphe de fédération de Mastodon, de la concentration des instances et de la fragilité opérationnelle sous modération au niveau des instances.

[32] Zignani, M., Gaito, S., & Rossi, G. P. (2018). *Suivez le « Mastodon » : structure et évolution d'un réseau social en ligne décentralisé .* Dans les Actes de la douzième conférence internationale de l'AAAI sur le Web et les médias sociaux (ICWSM 2018), Stanford, juin 2018. Analyse structurelle des débuts du réseau Mastodon, y compris le regroupement au niveau des instances et les propriétés du graphe de fédération.

[33] Open Data Institute. (octobre 2018). *Définition d'un « data trust ».* Document de travail de l'ODI. Établit la définition opérationnelle d'un data trust comme « une structure juridique assurant une gestion indépendante des données », reprise par la littérature politique et gouvernementale britannique ultérieure sur la conception institutionnelle de la gestion des données.

[34] Element AI / Nesta. (2019). *Data Trusts : un nouvel outil pour la gouvernance des données.* Recherche co-publiée sur la conception institutionnelle des trusts de données en tant que mécanisme visant à remédier aux asymétries de pouvoir entre les entreprises technologiques, le gouvernement et le public.

Auteur correspondant : John G. Stroh, directeur, My Digital Sovereignty Limited (NZ). ORCID : 0009-0005-2933-7170. E-mail : john.stroh@mysovereignty.digital.

Citation suggérée (sous réserve de l'accord de l'opérateur) : Stroh, J. G. (2026). *Architecture de registres souverains pour les plateformes à l'échelle communautaire — Document A.* My Digital Sovereignty Limited. (DOI Zenodo à attribuer lors de la publication.)

Statut du projet : projet de révision v4 — mai 2026. Commentaires et corrections bienvenus. Basé sur le rapport de mise en œuvre v0.4 précédent. La structure ajoute les sections « Travaux connexes », « Modèle de menace » et « Évaluation » conformément à l'étape C du plan de repositionnement du 01/05/2026. Article complémentaire (Article B — Couches linguistiques situées, synopsis de l'article empirique complémentaire, publié). Publié sur agenticgovernance.digital en tant que version préliminaire ; DOI Zenodo à attribuer au stade de la version candidate v4.