Sovereign-Record-architectuur voor platforms op gemeenschapsniveau

John G. Stroh

Paper A ·

Conceptversie v4, mei 2026 |

Talen: EN · DE · MI

HTML lezen PDF downloaden Bekijk diavoorstelling Feedback per e-mail

Inhoudelijke feedback over specifieke secties is welkom. Gelieve sectienummers te vermelden (bijv. §6.10) zodat correcties kunnen worden getraceerd. De auteur beantwoordt persoonlijk; houd rekening met een termijn van één tot twee weken. Het document is beschikbaar in het Engels, te reo Māori en Deutsch (links hierboven). De diavoorstelling is momenteel alleen in het Engels; gelokaliseerde diavoorstellingen volgen bij de v4 release-candidate.

Sovereign-Record-architectuur voor platforms op gemeenschapsnive Platforms

Cryptografische herkomst, tenant-gebonden beleidsafdwinging, bilaterale federatie en door leden aangestuurde soevereine overdraagbaarheid voor niet-hyperscaler-gemeenschapsinfrastructuur

John G. Stroh

03-05-2026

Sovereign-Record Architectuur voor platforms op gemeenschapsnive

Samenvatting

Het standaardplatform op gemeenschapsschaal is eigendom van een Amerikaans bedrijf, wordt gehost op door de VS gecontroleerde infrastructuur, levert geld op door middel van aandachtswinning en wordt beheerd volgens voorwaarden die de exploitant eenzijdig kan wijzigen. De alomtegenwoordigheid van het standaardplatform is geen op waarden gebaseerde overeenkomst die is bereikt door gemeenschappen die alternatieven tegen elkaar hebben afgewogen; het is het gevolg van meer dan een decennium van aanhoudende bedrijfsinvesteringen in het vormgeven van gebruikersverwachtingen, in lock-in-mechanismen op basis

van netwerkeffecten, en in het kaderen van het publieke discours waardoor alternatieven onpraktisch of onzichtbaar worden gemaakt. De omstandigheden blijven ononderbroken van kracht, ongeacht de instemming van de gemeenschap, en komen slechts af en toe aan het licht als zichtbare mislukkingen — een geblokkeerd account, een verwijderde post, een dienst die zonder voorafgaande kennisgeving wordt stopgezet, een herziening van de servicevoorwaarden die tegen het belang van de gemeenschap indruist. Voor sommige gemeenschappen — Māori taonga bewaren, minderheidstaalgemeenschappen waarvan de inhoud de taal zelf *is*, groepen voor familiegeschiedenis die gegevens bewaren van levende personen, en elke gemeenschap waarvan de levenswijze niet kan worden gereduceerd tot een profielobject — zijn die omstandigheden geen draaglijke ongemakken; het zijn structurele belemmeringen voor het werk waarvoor de gemeenschap bestaat. Dit artikel beschrijft een **architectuur voor soevereine records** — een alternatief substraat waarin de soevereiniteitseigenschappen die een gemeenschap nodig heeft inherent zijn aan de records zelf, en geen concessies zijn die de beheerder kan intrekken.

Elk inhoudsrecord in het systeem draagt zijn eigen herkomst, zijn eigen toegangsbeleid, zijn eigen versleutelingsidentificatie en een cryptografische keten van elke bestuursgrens die het heeft overschreden. Lezen legt deze status bloot aan consumenten; schrijven voegt eraan toe; verwijderingen maken er een tombstone van. Federatie tussen soevereine tenants is bilateraal en begrensd — twee gemeenschappen komen, op door hen gespecificeerde voorwaarden, één specifieke interactie overeen, en alleen die. Leden zijn eersteklas betrokkenen onder welk regelgevend kader dan ook dat op hen van toepassing is: elk mag de volledige set records waarin zij voorkomen in cryptografisch verifieerbare vorm exporteren, en migreren naar elke tenant die onder hetzelfde architecturale model opereert. Een begeleid dialoogplatform — door de operator goedgekeurde redactionele wachtrij, ontwerp-en-publicatiepoort, geen automatische publicatie, geen uitgaande berichten — breidt de alleen-lezen UI voor stakeholderbeheer uit naar participatief beheer zonder de discipline van toezicht op te geven.

De architectuur draait in productie op infrastructuur die onder de soevereiniteit van de EU (OVH Frankrijk) en Nieuw-Zeeland (Catalyst Cloud) valt. Er wordt gewerkt aan een carpool-configuratie als de eerste beoogde multi-instance federatie-implementatie. De bilaterale federatie- infrastructuur wordt end-to-end geleverd met een uitgebreide negatieve-test matrix die scope-gebonden leesbewerkingen, schrijfblokkering tussen tenants, volledigheid van auditlogs, citatiediscipline, caching/verouderingsgedrag, randgevallen van datastatussen, handhaving van autorisatiegrenzen, en resolutie van naamruimteconflicten omvat; live federatiekoppelingen tussen onafhankelijke tenants blijven in afwachting van de eerste multi-instance carpool- activering.

De architectuur is ontworpen om Te Tiriti-bestuursverplichtingen met betrekking tot AI-systemen die Māori gegevens gebruiken of produceren na te komen, in overeenstemming met de voorschrijvende principes van Dr. Taiuru Kaupapa Māori AI Framework [25b] (Māori -toestemming + gegevenssoevereiniteit over trainingsmateriaal + volledige verantwoordingsplicht). De meer open vraag die Dr. Taiuru [25a] stelt over rechtspersoonlijkheid voor AI-agenten die zijn samengesteld

uit Māori behoort tot het empirische domein van het begeleidende artikel (Artikel B — Situated Language Layers, samenvatting van het empirische begeleidende artikel, gepubliceerd) en wordt daar behandeld, niet in dit artikel. Een ontwikkelingskader (Tractatus, Apache 2.0) legt de architecturale consultaties vast die tot dit ontwerp hebben geleid; het permanente grootboek maakt deel uit van het evaluatieoppervlak. Het substraat is gebouwd door een klein team in Nieuw-Zeeland, zonder durfkapitaal. Het is een architectonisch antwoord op de vraag hoe gemeenschapsinfrastructuur de voorwaarden van de standaard soevereiniteit van Amerikaanse platforms kan weigeren zonder terug te krabbelen van het werk dat die infrastructuur verricht voor de gemeenschappen die zij bedient.

Sleutelwoorden: gegevenssoevereiniteit, isolatie van tenants, cryptografische herkomst, bilaterale federatie, rechten van betrokkenen, soevereine overdraagbaarheid, Te Tiriti o Waitangi, AI-persoonlijkheid, kaitiaki, beleidsopvolging, EUPL-1.2, CARE-principes, AVG artikel 15, Enhanced Border Security Partnership, CLOUD Act, gedecentraliseerde identificatoren.

---

1. Inleiding

Het standaardplatform op gemeenschapsniveau is een SaaS-instantie die eigendom is van een Amerikaanse onderneming, gehost wordt op door de VS gecontroleerde infrastructuur, geld oplevert door aandacht te genereren, en wordt beheerd door voorwaarden die de exploitant eenzijdig kan wijzigen. De alomtegenwoordigheid van het standaardplatform is niet het gevolg van een op waarden gebaseerde overeenkomst die is bereikt door individuele gebruikers of gemeenschappen die alternatieven tegen elkaar hebben afgewogen. Het is het gevolg van meer dan een decennium van aanhoudende bedrijfsinvesteringen in het vormgeven van gebruikersverwachtingen, in lock-in-mechanismen op basis van netwerkeffecten, en in het kader waardoor alternatieve regelingen onpraktisch of onzichtbaar worden gemaakt. De voorwaarden blijven ononderbroken van kracht, ongeacht de instemming van de gemeenschap, en komen slechts af en toe aan het licht als zichtbare mislukkingen — een geblokkeerd account, een verwijderde post, een dienst die zonder kennisgeving wordt stopgezet, een herziening van de servicevoorwaarden die tegen het belang van de gemeenschap indruist — terwijl de onderliggende regeling ononderbroken van kracht blijft. Voor sommige gemeenschappen — Māori die opereren onder Te Tiriti-verplichtingen, beroepsorganisaties waarvan de leden vertrouwelijk materiaal bezitten, stamboomgroepen die gegevens bewaren van levende personen bij naam, natuurbeschermingsgroepen waarvan de locatiegegevens gevoelig zijn, parochienetwerken, sportfederaties, minderheidstaalgemeenschappen en anderen wier levenswijze niet kan worden gereduceerd tot een profielobject — zijn de onderliggende voorwaarden onhoudbaar: het zijn structurele belemmeringen voor het werk waarvoor de gemeenschap bestaat.

Dit document is geschreven voor die gemeenschappen — en voor de bredere groep kleine organisaties die zij vertegenwoordigen: organisaties die vertrouwelijke informatie bewaren over infrastructuur buiten hun rechtsgebied, onder voorwaarden die alleen de exploitant kan herzien.

Drie factoren oefenen druk uit op deze gemeenschappen.

De eerste is **jurisdictioneel**. De CLOUD Act (2018) [9] breidt de Amerikaanse bevoegdheid tot het uitvaardigen van bevelen uit tot Amerikaanse cloudproviders wereldwijd, ongeacht waar de betrokkene woont. De onderhandelingen over het Enhanced Border Security Partnership (EBSP), die momenteel in de context van Nieuw-Zeeland in de publieke discussie zijn [13][14], zijn gekoppeld aan voortgezette deelname aan het Amerikaanse Visa Waiver Program, met een deadline voor de onderhandelende landen [13][14][15], en voorzien in uitgebreide toegang tot gegevens, waaronder biometrische en andere identiteitsinformatie [16][17]. In een juridisch commentaar van de Universiteit van Auckland [18] wordt opgemerkt dat de documentatie van het Amerikaanse Ministerie van Binnenlandse Veiligheid beschrijft dat de EBSP-afspraken aanzienlijk verder gaan dan de op individuele gevallen gebaseerde overdrachten in het kader van bestaande Passenger Name Record (PNR)-overeenkomsten, waardoor de mogelijkheid van directe toegang tot de database ontstaat. Privacy Foundation New Zealand heeft haar bezorgdheid geuit over transparantie en waarborgen [19]. Soevereiniteit is in deze context geen marketingterm: het is een kwestie van welk proces van welke staat openbaarmaking kan afdwingen, volgens welk tijdschema en met welke kennisgeving aan de gemeenschap waarvan de gegevens worden openbaar gemaakt.

Het tweede punt betreft **regelgeving**. Te Tiriti o Waitangi (het Verdrag van 1840 tussen de Kroon en Māori), de EU-AI-wet [6], de artikelen 9 en 15 van de AVG [8] en de Europese wet inzake mediavrijheid [7] leggen elk verplichtingen op aan de gegevensinfrastructuur van de gemeenschap die moeilijk of onmogelijk via delegatie kunnen worden nagekomen. Een platformbeheerder die niet kan aantonen welk model de inhoud van welk lid heeft geëvalueerd, aan de hand van welk door de gemeenschap opgesteld beleid, met welk besluit, kan niet voldoen aan de verplichtingen die deze instrumenten opleggen. Een platform dat niet in staat is om een lid, op verzoek, de volledige set records te leveren die het lid heeft aangemaakt in een verifieerbare vorm, kan niet voldoen aan het recht op inzage in AVG-artikel 15. Gemeenschappen die onder Te Tiriti opereren, hebben een overeenkomstige verplichting op grond van artikel 2 — rangatiraover taonga — die een architectuur structureel moet ondersteunen in plaats van alleen maar te verklaren.

De derde is **technisch**. De commodity AI-stack leidt inferentie via een klein aantal Amerikaanse infrastructuurproviders en behandelt de inhoud van elke gemeenschap als potentiële trainingsinput. Voor gemeenschappen waarvan de woordenschat, bestuursprotocollen of heilige materialen niet zonder schade kunnen worden gemiddeld in een wereldwijd corpus — en waarvan de verplichtingen uit hoofde van Te Tiriti of de CARE-principes door een dergelijke middeling zouden worden geschonden — is de commodity-stack onwerkbaar.

Dit artikel rapporteert een architectonisch antwoord. De centrale toezegging is concreet: elk inhoudsrecord draagt zijn eigen herkomst, zijn eigen toegangsbeleid en een cryptografische keten van elke bestuursgrens die het heeft overschreden. Lezen legt deze status bloot aan consumenten; schrijven voegt eraan toe; verwijderingen markeren het als verouderd. De architectuur draait in productie over meerdere 'village-type'-configuraties op infrastructuur die onder de soevereiniteit van de EU en Nieuw-Zeeland valt. Het werk is uitgevoerd zonder durfkapitaal, met het

budget van een klein team, door een particulier Nieuw-Zeelands bedrijf, met behulp van een governance-raamwerk voor de ontwikkelingstijd (Tractatus) dat zijn eigen architecturale beslissingen gaandeweg vastlegt.

Het artikel is als volgt opgebouwd. §2 schetst de achtergrond — het governancekader voor de ontwikkelingstijd, het Te Tiriti- en CARE-principes-kader voor inheemse gegevenssoevereiniteit (met Dr. Taiuru's(2026) tweeledige argument over Te Tiriti-verplichtingen en de open vraag over de rechtspersoonlijkheid van AI-agenten, besproken in §3.6), de operationele definitie van *soevereine records*, het bilaterale kader van federatie, en het 'lid-als-gegevenssubject'-kader voor soevereine overdraagbaarheid. §3 positioneert het werk ten opzichte van de verwante literatuur, inclusief de verhouding tot het argument vanDr. Taiuruals geciteerd gepubliceerd werk. §4 formaliseert het dreigingsmodel met benoemde tegenstanders en toetsbare predicaten. §5 beschrijft de ontwerpprincipes. §6 rapporteert de architecturale implementatie. §7 rapporteert federatie in productie. §8 rapporteert soevereine portabiliteit. §9 rapporteert de UI voor stakeholder-governance, inclusief het geleverde Phase-6-platform voor begeleide participatieve dialoog. §10 doorloopt een uitgewerkt voorbeeld van domeinoverschrijdende overdracht van naamgevingssoevereiniteit tussen twee gesitueerde taalmodules. §11 geeft een overzicht van de dorpachtige configuraties. §12 rapporteert de evaluatie. §13 beschrijft de open-sourcehouding. §14 vermeldt de architecturale bijdrage. §15 noemt wat de architectuur nog niet doet.

---

2. Achtergrond

2.1 Het Tractatus -framework

Het governance-mechanisme dat tijdens de ontwikkeling wordt gebruikt om het platform te bouwen en te exploiteren, is het Tractatus, een afzonderlijk onderzoeksproject van dezelfde auteur. Het framework bestaat uit een reeks architecturale patronen en codeservices voor AI-governance tijdens de ontwikkeling — voornamelijk services die ingrijpen in de besluitvorming van een AI-codeerassistent op architecturale keuzemomenten. Het framework is open source onder de Apache 2.0-licentie en wordt openbaar verspreid op `codeberg.org/mysovereignty/tractatus-framework` [1]. Een werkdocument documenteert de observatiebevindingen van het framework en de architecturale patronen die het codificeert; specifieke kwantitatieve cijfers worden gerapporteerd in het werkdocument in plaats van hier herhaald.

Tractatus is governance *tijdens de ontwikkeling*: het geeft vorm aan de broncode en architecturale keuzes van het platform, niet aan de verzoeken tijdens de uitvoering. Het platform raadpleegt het framework op architecturale beslissingspunten en slaat elke raadpleging op als een record in de platformdatabase; raadplegingen worden opgeslagen op basis van revisie-identificatie, dienst, voorwaardenlijst en PASS/FAIL-uitspraak. De discipline van het vastleggen van de raadpleging — uniform in lokale plus EU-soevereine en NZ-soevereine productiedatabases, geautomatiseerd door scripts per beslissing — is de bijdrage; een toekomstige lezer kan vragen welke voorwaarden een bepaalde architecturale beslissing betrof, en het antwoord staat in de database, niet in de tekst.

Het onderscheid is van belang. Tractatus is het raamwerk. Het platform is een toepassing daarvan. Dit artikel gaat over het platform; het raamwerk wordt ter volledigheid genoemd, aangezien de codebase van het platform er bij elk architectonisch beslissingspunt op terugvalt.

2.2 Te Tiriti o Waitangi en inheemse gegevenssoevereiniteit

Te Tiriti o Waitangi, het verdrag uit 1840 tussen de Britse Kroon en de Māori-iwi, vormt de basis van het Nieuw-Zeelandse constitutionele recht. De drie artikelen ervan — die de soevereiniteit van de stammen over taonga (kostbaarheden), het bestuurlijk gezag van de Kroon en gelijkwaardig burgerschap erkennen — vormen het kader voor hedendaagse verplichtingen met betrekking tot data. Het Waitangi Tribunal *WAI 262* -rapport [5] en de *CARE-principes voor inheems databeheer* [4] zijn veel geciteerde verwoordingen van wat deze verplichtingen betekenen voor de gegevensinfrastructuur van gemeenschappen. De CARE-principes — Collectief voordeel, Beheersingsbevoegdheid, Verantwoordelijkheid, Ethiek — zijn niet hetzelfde als de FAIR-principes voor open data; ze bestaan naast elkaar en hebben expliciet voorrang wanneer de twee met elkaar in conflict komen.

Een recenter rapport van het Tribunal, *WAI 2522* [13a], breidde de analyse uit naar internationale economische instrumenten — het Trans-Pacific Partnership-onderzoek, de bemiddelingsovereenkomst en de operationalisering van die instrumenten via het Ministerie van Buitenlandse Zaken en Handel. De conclusies van het Tribunaal in WAI 2522, samen met het werk van Ngā Toki Whakarururanga als platform voor dialoog Māori, scherpen de verplichting aan: een Kroon die Māori blootstelt aan een buitenlands rechtsstelsel — via verboden op gegevenslokalisatie in handelsverdragen, via blootstelling aan de CLOUD Act, of via een Enhanced Border Security Partnership dat directe toegang tot databases overweegt — kan niet voldoen aan de bescherming van taonga uit artikel 2, tenzij de architectuur zelf dergelijke blootstelling voorkomt. Architecturale soevereiniteit is de enige soevereiniteit die de toetsing van artikel 2 doorstaat zodra de eigen verdragsverplichtingen van de Kroon exportkanalen creëren.

Voor Māori hun rechten onder Te Tiriti doen gelden, moet een gemeenschapsplatform hen in staat stellen hun gegevens te bewaren op infrastructuur die zij kunnen controleren, beheerd volgens hun tikanga (gebruikelijke protocollen), zonder mogelijkheid tot toegang door andere gemeenschappen — inclusief door de platformbeheerder. De architectuur beantwoordt dit direct: isolatie van tenants is de fundamentele basis, geen functie. Een platformbeheerder met toegang op inhoudsniveau tot tenantgegevens kan niet voldoen aan de CARE-principeverplichting van *de Autoriteit om controle uit te oefenen*.

Dr. Karaitiana Taiuru (Ngāi Tahu, Ngāti Kahungunu) heeft uitgebreid gepubliceerd over Maori-technologie-ethiek, inheemse gegevenssoevereiniteit, AI- ethiek en digitale rechten; zijn werk is beschikbaar op taiuru.co.nz. De Village-taal-laag die op het hier beschreven platform draait, is getraind op basis van de gepubliceerde kaders vanDr. Taiuru, met zijn toestemming en onder vermelding van de bron. Dr. Taiuru’sbredere oeuvre op het gebied van Maori-AI-governance vormt het vaste referentiepunt voor het standpunt van dit artikel. Zijn Kaupapa Māori AI Framework [25b] (maart 2026), verwoord in de whakatauāki *He Tangata, He Karetao, He*

Ātārangi (een persoon, een marionet, een schaduw), benoemt Maori-toestemming en gegevenssoevereiniteit over kennis die wordt gebruikt bij AI- training, en volledige ketenverantwoordelijkheid bij ontwikkelaars, exploitanten en implementators, als vereiste praktijk gebaseerd op Te Tiriti en de VN Verklaring van de VN over de rechten van inheemse volkeren. De architecturale primitieven waarover dit artikel rapporteert, zijn ontworpen om aan die vereiste praktijken te voldoen. Dr . Taiuru'srecentere onderzoek [25a] stelt, afzonderlijk, de open vraag of en onder welke voorwaarden rechtspersoonlijkheid zou kunnen worden uitgebreid tot AI-agenten die zijn samengesteld uit Māori- kennis — voortbouwend op de WAI 2522-bevinding dat Māori-gegevens taonga zijn en op het precedent van de drie wetten inzake rechtspersonen met natuurlijke kenmerken (Te Urewera 2014; Te Awa Tupua 2017; Te Kāhui Tupua 2025) — een onderzoek dat hij uitdrukkelijk overlaat aan collectief werk tussen AI-ontwikkelaars, overheidsinstanties en Maori- gemeenschappen. Het onderzoek naar persoonlijkheid behoort tot het empirische domein van het bijbehorende Paper B (samenvatting van het empirische begeleidende artikel, gepubliceerd), waarin het architecturale patroon van de gesitueerde-taal-laag en de werkingsprincipes worden beschreven, en waarin het volledige empirische artikel in detail verslag zal doen van de cohorttrainingsdiscipline waarop elke toekomstige partnerschapsbetrokkenheid per cohort (inclusief met Meads Tikanga-test) zou voortbouwen; dit artikel loopt niet vooruit op dat werk.

De architectuur gaat niet specifiek uit van Māori. De zelfde eigenschap — een platform dat niet over gemeenschappen heen kan kijken — beantwoordt aan de wettelijke verplichtingen waarmee EU-minderheidstaalgemeenschappen worden geconfronteerd onder de Europese Media Freedom Act en de speciale categorie-bescherming van artikel 9 van de AVG, waarbij culturele gegevens van minderheidstalen aannemelijk kunnen worden opgevat als een speciale categorie. Een Welshe gemeenschap, een Sámi-gemeenschap, een Sorbische gemeenschap, een Friese gemeenschap, een Catalaanse gemeenschap kan dezelfde architectuur overnemen door de taallaag opnieuw te trainen op een ander corpus en het beleid opnieuw op te stellen binnen hun eigen wettelijk kader; de architectuur zelf is overdraagbaar. Deze overdraagbaarheid is een centraal architectonisch kenmerk.

2.3 Waarom "soevereine records" in plaats van "versleuteld in rust"

De term *soeverein record* is bewust gekozen. Versleuteling in rust is een functie; soevereiniteit is een architectonische eigenschap. Een record is soeverein in de hier bedoelde zin wanneer aan elk van de volgende voorwaarden is voldaan:

1. Het draagt zijn eigen herkomst — wie het heeft geschreven, wie de kaitiaki(beheerder) is, onder welke tikanga het werd gedeeld, wanneer het werd gemaakt, en een cryptografische hash die deze velden aan elkaar bindt.
2. Het draagt zijn eigen beleid — wie het kan lezen, wie ermee kan trainen, wie het kan exporteren, wat er gebeurt bij beleidsconflicten.
3. Het draagt zijn eigen bewijsketen met zich mee — elke governancegrens die het heeft overschreden (aanmaak, update, export, verwijdering) wordt vastgelegd met een cryptografische handtekening.
4. De cache van de verificatiestatus is zichtbaar op het moment van lezen — elke API-gebruiker ziet of de keten van het record actueel, verlopen, niet-

overeenkomend of niet-verifieerbaar is, zonder dat hij het platform op zijn woord hoeft te geloven.

5. Het is overdraagbaar op verzoek van een lid. Een lid mag de volledige set records exporteren waarvan hij de auteur, de kaitiaki of anderszins als betrokkene wordt genoemd; de export draagt de bewijsketen voort; een externe verificateur die in het bezit is van het gepubliceerde identificatiedocument van de brontehuurder kan elke ondertekende vermelding in de records reconstrueren.

Dit zijn operationele eigenschappen, die vanuit de API-interface kunnen worden getest, en geen ambitieuze eigenschappen. In de rest van dit document wordt beschreven hoe elk van deze eigenschappen is opgebouwd.

2.4 Federatie: bilateraal en begrensd

Een federatie in de zin van het platform is de enge technische regeling die twee soevereine tenant-instanties in staat stelt verbinding te maken voor specifieke, afgebakende doeleinden — gezamenlijke evenementen, gedeelde carpoolen, instantieoverschrijdende aankondigingen — zonder dat een van beide gegevens, identiteit of bestuursbevoegdheid afstaat. Een federatie is een bilaterale overeenkomst: de statuten van de twee tenants komen overeen, de twee operators komen overeen, het federatiemanifest wordt door beide ondertekend. Er is geen centrale federatieserver; de gegevensstroom is direct, het bestuur is lokaal en elke partij kan de federatie op elk moment opzeggen.

Dit verschilt structureel van het platformmodel, waarbij instanties bladeren zijn aan de boom van één enkele operator. Het verschilt ook structureel van het dominante fediverse-model, waarbij federatie een netwerkbrede eigenschap is die wordt bemiddeld door een gedeeld protocol tussen door operators gecontroleerde servers. De hier beschreven architectuur is bilateraal en afgebakend: twee gemeenschappen komen overeen, op door hen gespecificeerde voorwaarden, om een specifieke interactie aan te gaan, en alleen dat.

§3 zet dit af tegen de verwante literatuur. §7 rapporteert over de federatie-infrastructuur die is geleverd en de status van de live-implementatie . §10 geeft een uitgewerkt voorbeeld van een bilaterale federatie tussen een botanische-kennismodule en een taalrevitalisatiemodule — een soort federatie die wordt overwogen voor curriculumintegratie in basisschoolomgevingen.

2.5 Het lid als betrokkene

Een lid van een tenant met soevereine gegevens is tegelijkertijd lid van de gemeenschap (met de sociale, bestuurlijke en inhoudscreatierechten die het lidmaatschap met zich meebrengt) en een betrokkene onder de regelgevende kaders die op hen van toepassing zijn. Een lid van de Welshe taalgemeenschap is een betrokkene in de zin van de AVG; de gegevens van een lid Māori vallen zowel onder de Te Tiriti-rechten van de iwi als onder de AVG-rechten van het individu wanneer de iwi door de EU gehoste infrastructuur exploiteert voor leden van de diaspora; een lid van een Duitse Verein is zonder meer een betrokkene in de zin van de AVG.

De architectuur behandelt het kader van het lid als betrokkene als eersteklas. Het

`metadata.origin` -blok van elk record noemt de auteur en (indien verschillend) de kaitiaki, beide als gedecentraliseerde identificatoren. `Het metadata.policy-blok` van elk record geeft aan of en hoe dat record mag worden gedeeld, gebruikt voor training of geëxporteerd, en beleidsconflicten worden opgelost via de constitutionele standaardinstelling. Door leden aangestuurde export (§8) neemt het beleid letterlijk: het beleid van een record kan de export ervan verbieden, zelfs door de auteur (bijv. een beraadslaging bijgedragen onder voorwaarden van collectieve toestemming), en de export-wrapper dwingt dit af. Soevereiniteit is geen tegenstelling tussen lid en collectief; het is het architecturale kader waarbinnen beide rechten naast elkaar bestaan, en het kader maakt het conflict expliciet in plaats van het te verbergen in implementatiekeuzes.

---

3. Gerelateerd werk

De architectuur bevindt zich op het snijvlak van verschillende actieve onderzoeks- en ontwikkelingslijnen. Positionering is cruciaal omdat de bijdrage niet de introductie is van een enkele primitieve — bekende bouwstenen worden hergebruikt — maar de integratie van die primitieven in een substraat dat het dreigingsmodel in §4 beantwoordt vanaf het recordniveau omhoog in plaats van vanaf het operatorniveau naar beneden.

De literatuurstudie die volgt in §§3.1–3.7 plaatst de doelstellingen van dit artikel in de context van aanverwant onderzoek. Lezers die zich richten op governance-argumenten kunnen doorgaan naar §7 (federatie in productie), §8 (soevereine overdraagbaarheid) of §9 (stakeholder-governance-UI) met de conclusie dat de primitieven van de architectuur — bilaterale federatie, soevereine overdraagbaarheid, cryptografische verwijderingsmechanismen die een compromittering van de operator overleven — zijn ontworpen om runtime-omzeiling te weerstaan onder het dreigingsmodel in §4. De onderstaande literatuur geeft aan hoe elke primitieve zich verhoudt tot zijn naaste buur in het gepubliceerde onderzoek.

3.1 Gefedereerde sociale infrastructuur

ActivityPub [Snell & Prodromou, 2018, W3C-aanbeveling [20]] en het Mastodon-ecosysteem stellen federatie vast als een netwerkbrede eigenschap, bemiddeld door een gedeeld protocol tussen door operators gecontroleerde servers. In ActivityPub-federatie federeren twee servers door het uitwisselen van ondertekende activiteitsobjecten; de granulariteit is per actor en per activiteit, bemiddeld door de verzamel-eindpunten van het protocol. Dit verschilt structureel van de hier beschreven bilaterale en begrensde federatie. De bijdrage van ActivityPub is interoperabiliteit tussen duizenden instanties; de bijdrage van dit artikel is het behoud van soevereiniteit tussen precies twee instanties tegelijk, via een ondertekend manifest, met intrekking als een eersteklas bewerking. Beide architecturen zijn geldige antwoorden op verschillende soevereiniteitsstandpunten: ActivityPub optimaliseert voor grafiekbereik; dit artikel optimaliseert voor tribale/collectieve autoriteit over de federatie- envelop.

De literatuur over gedecentraliseerde sociale media documenteert eigenschappen van federatiegrafieken, afwegingen bij moderatie op instantieniveau en hiaten in de overdraagbaarheid van inhoud. Empirische karakteriseringen van de Mastodon-grafiek en patronen van instantiemoderatie [31][32] vormen de basis voor de operationele analyse van fediverse-platforms; later werk aan het AT-protocol [Bluesky Public Benefit Corporation, 2024 [21]] stelde accountportabiliteit voor — de gegevens van een lid volgen het lid in plaats van de server — als een structureel antwoord op het moderatie- en vindbaarheidsprobleem. De soevereine overdraagbaarheid in dit artikel (§8) is technisch verwant, maar heeft een andere drijfveer: overdraagbaarheid is een recht van de betrokkene op grond van artikel 15 van de AVG, en de grondwettelijke acceptatiecontrole door de ontvangende tenant (§8) is integraal, niet optioneel. De overdraagbaarheid van het AT-protocol is accountgedreven; de overdraagbaarheid in dit document is recordgedreven en respecteert het beleid, met een manifest met een lijst van achtergehouden records waarvan het beleid export verbiedt, zelfs door de auteur ervan.

3.2 Gedecentraliseerde identificatoren en verifieerbare referenties

De W3C Decentralized Identifiers (DID's) v1.0-specificatie [11] stelt een methode-agnostisch identificatieschema vast dat meerdere resolutiemechanismen ondersteunt. De tenants en leden van het platform publiceren DID- documenten op bekende eindpunten onder het eigen domein van de tenant; verificatie van cryptografische bewerkingen (herkomst-hashes, proof-chain- handtekeningen, federatiemanifesten, exportbundels) wordt uitgevoerd aan de hand van deze documenten. Dit patroon volgt de conventie die wordt gebruikt in het verwante werk dat wordt aangehaald in §§3.1–3.7; de architecturale beslissing is om elke cryptografische bewerking in het systeem onafhankelijk verifieerbaar te maken met behulp van alleen het gepubliceerde DID-document van de brontehuurder en standaard cryptografische primitieven — geen externe verificateur, geen gedeelde vertrouwenswortel, geen gecentraliseerd register.

3.3 Solide en persoonlijke gegevensopslagplaatsen

Solid [Mansour et al., 2016 [22]; W3C Solid Community Group] en het Inrupt-platform slaan gegevens op in persoonlijke pods die eigendom zijn van de betrokkene, waarbij applicaties toegang aanvragen via WebID-gebaseerde autorisatie. Solid richt zich architectonisch op *gegevens per individu*; dit artikel richt zich op *gegevens per gemeenschap, waarbij leden eersteklas betrokkenen binnen de gemeenschap zijn*. De twee vullen elkaar aan in plaats van met elkaar te concurreren: een Solid-pod zou in principe kunnen dienen als exportbestemming voor een bundel soevereine records, en een gemeenschap waarvan de leden elk Solid-pods onderhouden, zou in principe de soevereine recordtenant van het platform daarbovenop kunnen implementeren. De keuze van het platform om de *gemeenschapseenheid* centraal te stellen weerspiegelt een inhoudelijk standpunt dat minderheidstaal- en inheemse gemeenschappen geen verzamelingen zijn van individuele gegevenssubjecten: het collectief is de rechthebbende op taonga (CARE-principe: Collectief voordeel), en de architectuur moet de autoriteit van het collectief dienen (Autoriteit om te controleren).

3.4 Federatief leren en datatrusts

Federated learning [McMahan et al., 2017 [23]; Kairouz et al., 2021 survey [24]] *verschilt architectonisch* van dit werk. Federated learning traint een gedeeld model door gradiëntupdates uit te wisselen tussen partijen die gegevens bewaren, zonder ruwe gegevens uit te wisselen. De federatie in dit artikel wisselt helemaal geen modelparameters uit — federatie is een gegevensovereenkomst tussen tenants onder een ondertekend manifest, waarbij de gegevensstroom per overeenkomst wordt gedefinieerd en er geen gedeeld model wordt geïmpliceerd. De situatietaal-laag van het platform is per definitie per tenant; het delen van modelparameters tussen tenants zou in strijd zijn met de fundamentele primitieve van tenant-isolatie (§5.1). Empirisch bewijs uit de trainingsdiscipline voor de situated-language-laag wordt apart gepresenteerd in Paper B (samenvatting van het empirische begeleidende artikel, gepubliceerd).

Datatrusts — zoals ontwikkeld in de werkdefinitie van het Open Data Institute van een datatrust als “een juridische structuur die zorgt voor onafhankelijk beheer van gegevens” [33] en het parallelle onderzoek van Element AI naar het institutionele ontwerp van datatrusts als mechanisme om machtsongelijkheid tussen technologiebedrijven, de overheid en het publiek aan te pakken [34] — introduceert een derde partij als trustee die gegevens namens een gemeenschap bewaart en toegang bemiddelt. De architectuur van dit artikel kent geen dergelijke trustee. De platformbeheerder kan infrastructuuractiviteiten uitvoeren (tenants aanmaken, facturering beheren, de status bewaken), maar kan de inhoud van tenants niet lezen. Er is geen rol in het systeem die gegevens van verschillende tenants samenvoegt, zelfs niet tijdelijk. De kracht van een datatrust is institutionele bemiddeling; de kracht van deze architectuur is de onmogelijkheid van bemiddeling vanuit het platform zelf.

3.5 Implementatie van artikel 15/20 van de AVG Het

Het recht op inzage (artikel 15) en het recht op gegevensoverdraagbaarheid (artikel 20) van de Algemene Verordening Gegevensbescherming [8] hebben een omvangrijke implementatieliteratuur — waaronder Wachter, Mittelstadt & Floridi [26] over het debat over uitlegrechten, en Edwards & Veale [27], die betoogt dat het recht op verwijdering (artikel 17) en gegevens overdraagbaarheid (artikel 20) meer praktisch gewicht in de schaal leggen dan uitlegrechten voor algoritmische verantwoordingsplicht. Het DSR-eindpunt van het platform (§8) implementeert alle zes relevante rechten (artikelen 15, 16, 17, 18, 20, 21) via een uniforme exportpijplijn voor soevereine records die de records van de betrokkene retourneert met volledig behoud van de proof-chain, in JSON-, CSV- of PDF-formaten, als één canonieke bundel. De technische nieuwigheid hier is de *cryptografische verifieerbaarheid* van de bundel: elke externe partij met het gepubliceerde DID-document van de brontehuurder kan elke vermelding in de records van de bundel verifiëren, zonder vertrouwen te stellen in de brontehuurder of de door de betrokkene gekozen ontvangende partij. Standaard implementaties van artikel 15 leveren gegevens op; deze implementatie levert *verifieerbare* gegevens op.

3.6 CARE Principes en inheems gegevensbeheer

De CARE-principes [4] vormen het kader voor een inhoudelijke verplichting die architecturale implicaties heeft: *bevoegdheid tot controle* vereist dat de gemeenschap — niet de platformbeheerder, niet een externe beheerder, niet een toezichthouder met dagvaardingsbevoegdheid buiten het rechtsgebied van de gemeenschap — de gegevens op haar eigen voorwaarden kan beheren. Vervolgwerk op het gebied van inheems gegevensbeheer — Walter & Suina [25] over inheemse gegevens en methodologieën; Te Mana Raraunga *Principles of Māori Data Sovereignty* [28]; Carroll, Rodriguez-Lonebear & Martinez [29] over strategieën van inheemse volkeren in de VS; Hudson, Anderson, Dewes, Temara, Whaanga & Roa [30] over het conceptualiseren van big data door een Māori — heeft de implicaties voor de gehele levenscyclus van gegevens (verzameling, opslag, verwerking, delen, archivering) uitgewerkt. De architecturale keuze van het platform — tenant-isolatie als basis, soevereine records als substraat, bilaterale federatie als het enige cross-tenant-mechanisme — is één technisch antwoord op de CARE-verplichtingen; het is niet het enige mogelijke antwoord, maar het is een architecturaal antwoord dat de toetsing van artikel 2 van Te Tiriti doorstaat in het specifieke geval van Nieuw-Zeelandse iwi en jurisdictionele druk van de EBSP-klasse.

Dr. Taiuruwerk op het gebied van Māori AI-governance [25a, 25b] (geïntroduceerd in §2.2) scherpt de CARE-verplichtingen aan tot specifieke architecturale toezeggingen. De prescriptieve plicht — Māori -toestemming en gegevenssoevereiniteit over kennis die wordt gebruikt bij AI-training, volledige ketenverantwoordelijkheid bij ontwikkelaars en exploitanten, en Te Tiriti-verplichtingen voor AI-systemen die Māori gegevens gebruiken of produceren — geldt nu voor elk platform waarvan de AI-toepassingen in aanraking komen met taonga materiaal. De architecturale primitieven die in dit document worden beschreven (tenant-isolatie als rangatiraover gegevens volgens Artikel II; cohorttraining per tenant als de locus van door de gemeenschap bepaald modelgedrag voor tenantsMāori; de geleverde Phase-6 superviseerde dialooginterface (§9) als kaitiaki op wat de interface uitzendt; definitieve cryptografische verwijdering als rangatiraover wat vergeten wordt; DID-gebaseerde attributie en de bewijsketen als whakapapa traceerbaarheid van elk record) zijn bedoeld als een structureel antwoord op die prescriptieve plicht. De verdere vraag die Dr. Taiuru [25a] stelt — of en onder welke voorwaarden rechtspersoonlijkheid zou kunnen worden uitgebreid tot AI-agenten die zijn samengesteld uit Māori, naar het voorbeeld van Te Urewera (2014), Te Awa Tupua (2017) en Te Kāhui Tupua (2025) — wordt behandeld in het bijbehorende Paper B op het niveau van cohorttraining, en wordt niet vooraf behandeld in dit document.

3.7 Aangrenzende bedreigingen: buitenlandse cloudmining via grensverleggende AI

In commentaar uit de industrie op soevereine AI-architectuur [22b][23b][24b] is de convergentie geanalyseerd van Amerikaanse wettelijke toegangskaders (CLOUD Act; FISA) en de inzet van grensverleggende AI-modellen op door de VS gecontroleerde cloudinfrastructuur als een gecombineerd risicopad: gegevens die onder buitenlandse wettelijke dwang worden geraadpleegd, kunnen op grote schaal door grensverleggende AI-modellen worden gemined op patronen

die het oorspronkelijke openbaarmakingsbereik overschrijden. De implicaties voor biometrische, identiteits- en authenticatiegegevens zijn bijzonder groot. De architecturale oplossing die dit document voorstelt, is dat kritieke inloggegevens en biometrische gegevens in de eerste plaats nooit in buitenlandse cloudinfrastructuur worden opgeslagen, en dat elke LLM-interactie met soevereine gegevens verloopt via een door de tenant beheerde interface, waarbij de tenant beperkt wat een extern model kan leren of bewaren.

---

4. Bedreigingsmodel

In dit hoofdstuk worden de bedreigingen geformaliseerd waartegen de architectuur is ontworpen om weerstand te bieden. Het model noemt zes tegenstanders, vermeldt de soevereiniteits invarianten die elk niet mogen worden geschonden, en zet elke invariant om in een toetsbaar predikaat.

4.1 Tegenstanders

A1. Hostoperator gedwongen door jurisdictie. Een platformoperator die zelf gedwongen wordt door een buitenlands rechtsstelsel — een CLOUD Act-bevel, een FISA-bevel, een bepaling inzake databasetoegang van het Enhanced Border Security Partnership, een gelijkwaardige bepaling onder een andere jurisdictie — om gegevens van tenants openbaar te maken waartoe zij technisch toegang hebben. De dwang kan gepaard gaan met een spreekverbod. De beheerder kan te goeder trouw, te kwader trouw of onder dwang handelen; de architectuur staat los van het motief van de beheerder en gaat uit van het ergste scenario. De categorie tegenstanders is niet hypothetisch: zie bijvoorbeeld de datalek bij Instructure / Canvas in mei 2026, waarbij ongeveer 275 miljoen records van 8.809 onderwijsinstellingen werden gestolen bij één enkele edtech-exploitant (uitgebreide berichtgeving onder meer door Malwarebytes, TechCrunch en SecurityWeek; de aanval werd opgeëist door de groep ShinyHunters; Instructure bevestigde de ongeoorloofde toegang).

A2. Medehuurder. Een andere huurder op dezelfde platforminfrastructuur die probeert inhoud te lezen die niet van hem is, hetzij via queryconstructie, schemakennis, rol-escalatie of het misbruiken van een gedeelde bron (database, cache, bestandssysteem).

A3. Cross-tenant federatiepartner. De tenant aan de andere kant van een bilaterale federatieovereenkomst, die toegang probeert te krijgen tot gegevens buiten het afgebakende doel van het manifest, of wiens eigen infrastructuur zelf juridisch gecompromitteerd is (chain-of-trust-aanval via federatie).

A4. Lid-als-aanvaller. Een lid van een tenant die toegang probeert te krijgen tot inhoud die hij niet mag lezen (bijv. de besloten beraadslagingen van een ander lid, een voor een subgroep beperkt record waarvan hij geen lid is), of die probeert autoriteit uit te oefenen die hij niet bezit (bijv. een tenant-admin-bewerking uitvoeren, de statuten wijzigen).

A5. Buitenlandse cloud-mining via grens-AI. Een tegenstander die via A1 toegang

tot gegevens heeft afgedwongen en de gegevens vervolgens door een grens-AI-model leidt om patronen te extraheren die het wettelijke bereik van de oorspronkelijke openbaarmaking overschrijden — biometrische correlatie tussen populaties, afleiding van authenticatiepatronen uit sessiemetadata, reconstructie van sociale grafieken op basis van interactiesporen.

A6. Tegenstander die gebruikmaakt van biometrische gegevens. Een tegenstander die, door een combinatie van A1 (juridisch gedwongen host) en A5 (buitenlandse cloud-mining via grens-AI), tracht biometrische gegevens die door het platform worden bewaard — gezichten, vingerafdrukken, stemprofielen, irisscans, gedragsbiometrische profielen — te exploiteren om leden te identificeren, te correleren of te dwingen. De invloed van de tegenstander neemt toe met de onherroepelijkheid van biometrische gegevens: een gelekt wachtwoord kan worden gewijzigd, een gelekte gezichtsafdruk niet. Het bereik van de tegenstander wordt versterkt door de drie samenkomende blootstellingsroutes voor biometrische gegevens onder Amerikaanse jurisdictie — directe registratie aan Amerikaanse zijde bij grenzen en visuminterviews, hosting in Amerikaanse clouds onder dwang van de CLOUD Act, en toekomstige Enhanced Border Security Partnership-afspraken die directe databasetoegang tot biometrische opslagplaatsen van partnerlanden overwegen. Het architecturale antwoord is dat het platform geen enkel soort biometrische gegevens bewaart in enig pad dat het beheert (zie §5 ontwerpprincipes en §13.1 leveranciersdiscipline).

A7. Verkeerde toeschrijving via aggregerende agent. Een toekomstig agentoppervlak — runtime, persistent, doelgericht — dat inhoud aggregeert over tenants heen of over records binnen een tenant op manieren die ontsnappen aan `het share_within-beleid` per record ofde kaitiaki-attributie per record; of dat emergente attributies (auteurschap, kaitiakitanga, tikanga-dragende relaties) produceert die de onderliggende records niet rechtvaardigen. De runtime van het platform omvat vandaag een single-turn situated-language-layer dispatch (§5 ontwerpprincipes) en het geleverde Phase-6 mdsl participatieve dialoogoppervlak (§9), dat zelf onder toezicht staat van een single-turn — door de operator gekoorde redactionele wachtrij, een gate voor opstellen en publiceren, geen automatische publicatie, geen uitgaande berichten. Geen van beide biedt het volledige technische mechanisme van A7 (autonomie + persistentie + cross-record aggregatie). De Te Tiriti-governanceplicht die Dr. Taiuru (2026) stelt (zie §3.6) heeft betrekking op de substantiële last van deze tegenstander — namelijk dat elke cross-record of cross-tenant emissie van een Māori-dragende tenant de plicht draagt, ongeacht het autonomieniveau van het oppervlak. De bestaande invariant I3 van de architectuur (beleidconforme openbaarmaking) is de primaire technische verdediging: elke emissie tussen records of tenants wordt aan de routegrens aan het beleid getoetst; kaitiaki-attributie en de bewijsketen zorgen voor whakapapa-traceerbaarheid door elk record; de Phase-6 redactionele wachtrij + ontwerp-en-publiceerpoort (gemodelleerd naar het Mastodon-precedent van 'alleen publiceren op instructie') is de discipline tegen het stilzwijgend ontstaan van gedragingen in sterkere zin vanuit de gesuperviseerde basislijn. Het overnemen van het bredere advies vanDr. Taiuru— dat naleving van tikanga veel gemakkelijker vanaf het begin kan worden ingebouwd dan achteraf — wordt A7 hier genoemd zodat elke toekomstige stap naar autonomie of persistentie de weigeringseigenschap erft als een ontwerp-invariantie in plaats van een corrigerende patch.

4.2 Soevereiniteitsinvarianten

Voor elke tegenstander verdedigt de architectuur een of meer invarianten:

I1. Isolatie van tenant-inhoud. Geen enkele platformbeheerder, geen enkele medetentant en geen enkel geautomatiseerd proces buiten de eigen verzoekcontext van de tenant kan de inhoud van de tenant lezen. (Biedt bescherming tegen A1, A2.)

I2. Authenticiteit van herkomst. De auteur en kaitiaki van elk inhoudsrecord zijn cryptografisch gebonden aan de inhoud van het record; geen van beide velden kan stilzwijgend worden gewijzigd zonder de verificatiecache ongeldig te maken. (Beschermt tegen A1, A4.)

I3. Beleidsconforme openbaarmaking. Elke gegevensstroom tussen tenants of over grenzen heen respecteert de `metadata.policy.share_within` van het record en het afgebakende doel van het federatiemanifest; stromen buiten die omhulling worden geweigerd bij de routegrens. (Beschermt tegen A1, A3.)

I4. Definitiefheid van cryptografische verwijdering. Records waarvan `metadata.policy.delete` is ingesteld, kunnen worden verwijderd op een manier die de versleutelde tekst onherstelbaar maakt vanuit de opgeslagen toestand, zelfs voor de platformbeheerder met volledige databasetoegang . (Beschermt tegen A1, A5.)

I5. Integriteit van het federatiemanifest. Een bilaterale federatie wordt pas geactiveerd nadat de handtekeningen van beide partijen zijn geverifieerd aan de hand van hun respectievelijke gepubliceerde DID-documenten; intrekking is zelf een ondertekende gebeurtenis; geen enkele derde partij kan een federatie via een achterdeur binnendringen. (Beschermt tegen A3.)

I6. Reconstrueerbaarheid bij audits. Elke grensoverschrijdende gebeurtenis (aanmaken, bijwerken, exporteren, verwijderen, activering van federatie, intrekking van federatie, wijziging van lidmaatschap) laat een ondertekende proof-chain-vermelding achter; de tenant kan elke gebeurtenis reconstrueren vanuit zijn eigen database zonder te vertrouwen op de bewering van de platformbeheerder. (Beschermt tegen A1, A3.)

I7. Eerlijkheid inzake soevereine overdraagbaarheid. De export van toegangsrechten van een lid wordt gefilterd door dezelfde beleidsgate die gewone leesbewerkingen regelt; records waarvan het beleid export verbiedt, worden in het exportmanifest vermeld als achtergehouden, met vermelding van de beleidsreden. (Beschermt tegen A4 en waarborgt het vermogen van A1 om te beweren: “we hebben aan de betrokkene alles geëxporteerd waarop hij recht had.”)

I8. Beperking van off-platform-mining. Geen enkel inhoudsrecord verlaat de database van de tenant in leesbare tekstvorm, behalve via een route die is getoetst aan de grondwet van de tenant; runtime AI- inferentie (gesitueerde taallaag) wordt uitgevoerd op door de tenant gecontroleerde infrastructuur met beleidsgestuurde invoer. (Beschermt tegen A5.)

I9. Geen verzameling van biometrische gegevens. Het platform verzamelt, slaat op en verwerkt geen enkele vorm van biometrische gegevens in enig pad dat het beheert — geen gezichtsafdrukken, geen vingerafdrukken, geen stemafdrukken, geen irissjablonen, geen gedragsbiometrische profielen, geen van biometrische gegevens

afgeleide sleutels. (Beschermt tegen A6; versterkt A1 — de operator kan niet worden gedwongen om openbaar te maken wat nooit is verzameld; versterkt A5 — er bestaat geen biometrisch miningoppervlak.)

4.3 Testbare predicaten

Elke invariant leidt tot een of meer predicaten die testbaar zijn vanuit de API-interface of door directe inspectie van de database.

Voor I1 (isolatie van tenant-inhoud): alle query's van verzamelingen op tenant-niveau zijn zo opgebouwd dat het weglaten van een tenant-filter een runtime-fout veroorzaakt; een geautomatiseerde testsuite controleert dit. De `op AsyncLocalStorage gebaseerde` request-context-plugin van het platform dwingt het predikaat af; query's buiten de request- context (geplande taken, batch-jobs) moeten zich expliciet afmelden en documenteren waarom.

Voor I2 (authenticiteit van herkomst): voor elk record `r`, `recompute_provenance_hash(r.metada` `== r.metadata.origin.provenance_hash`; de serialisatie in canonieke vorm is stabiel in hydratatiemodus (een incident op 22-04-2026 , waarbij 25 unit-tests vlekkeloos werden doorlopen terwijl de hashes van echte Mongoose-documenten afweken van die op het moment van opslaan, bracht deze vereiste aan het licht). Use-case-validatie (§12) bevestigt de stabiliteit van de hash in alle hydratiemodi.

Voor I3 (beleidconforme openbaarmaking): voor elke uitzending over verschillende routes of WebSockets wordt de effective-policy-gate aangeroepen; een record waarvan `de share_within-` waarde niet voorkomt in de erkende woordenschat, faalt met de status CLOSED en de reden `share_within_unknown_scope`; dit is het project's *'wees eerlijk over wat niet kan worden geverifieerd; creëer geen toestemmingshouding uit het niets*'. Een geautomatiseerde test bouwt federatie-peer-scenario's op en controleert het gedrag van de gate voor elk scenario.

Voor I4 (definitiefheid van cryptografische verwijdering): voor elk record gemarkeerd `met delete_must_be_cryptographic` vernietigt verwijdering de versleutelingssleutel per record in de sleutelopslag van de tenant; volgende leespogingen retourneren `unverifiable` in plaats van `valid`; de versleutelde tekst in rust is niet herstelbaar door herversleuteling.

Voor I5 (integriteit van het federatiemanifest): een federatiemanifest bevat handtekeningen van beide partijen; `verify_signature(manifest, party_a.did_document) == true && verify_signature(manifest, party_b.did_document) == true`; de federatie wordt niet geactiveerd als een van beide mislukt; een statische test controleert of geen enkel codepad de federatie activeert zonder deze controles.

Voor I6 (reconstrueerbaarheid van audits): voor elke tenant-gebonden reeks gebeurtenissen kan de bewijsketen voor elk betrokken record worden gereconstrueerd door de ondertekende vermeldingen te lezen; geen enkele gebeurtenis is stil; de auditlog-schrijver van de architectuur wordt aangeroepen vanuit één enkel knelpunt dat niet kan worden omzeild door een controller die de aanroep overslaat.

Voor I7 (eerlijkheid van soevereine overdraagbaarheid): voor een exportverzoek

op grond van artikel 15 bevat het antwoord (a) de canonieke bundel, (b) de lijst met achtergehouden gegevens waarin elk uitgesloten record en de beleidsreden daarvoor worden genoemd, (c) een ondertekend ontvangstbewijs dat beide omvat. Een integratietest bevestigt dat achtergehouden records zijn uitgesloten *en* vermeld.

Voor I8 (beperking van off-platform-mining): de runtime inferentielayer wordt gehost op door de tenant gecontroleerde of door de gemeenschap vertrouwde infrastructuur (in het geval van het platform, EU-soevereine OVH France of door Nieuw-Zeeland beheerde Catalyst Cloud, of een aangewezen home-eGPU-failover). Er is geen verzoek aan een door de VS beheerd inferentie-eindpunt in het productie-verzoekpad. Een leveranciersverbodsregel, afgedwongen door codereview, somt toegestane en verboden providers expliciet op.

Voor I9 (geen verzameling van biometrische gegevens): een code-grep tegen de broncodeboom van het platform levert nul overeenkomsten op voor bibliotheek- of API-namen voor biometrische gegevensverwerking; een runtime-probe van de gegevensopslagplaatsen van het platform levert geen velden op die op biometrische gegevens lijken; een statische test bevestigt dat er nergens in de broncode van het platform een bibliotheek voor biometrische gegevensverwerking is geïmporteerd. De architecturale toezegging is vastgelegd in de regel inzake leveranciersverbod (§13.1) en wordt bij elke wijziging geverifieerd door middel van codereview. Het lokaal op het apparaat van het lid ontgrendelen met biometrische gegevens van een door het lid beheerde credential vault — Apple Secure Enclave, Android StrongBox, hardware-token vaults — is toegestaan en architecturaal onzichtbaar voor het platform; de biometrische gegevens overschrijden nooit de grenzen van het platform.

Het dreigingsmodel is niet uitputtend. Het is het model waarvan *bekend* is dat de architectuur het verdedigt, met benoemde predicaten die de operator en externe auditors kunnen testen. Dreigingen die hierboven niet zijn opgesomd (deniable-encryption-aanvallen, side-channel-aanvallen op de sleutelopslag , supply-chain-aanvallen op het Tractatus) vallen buiten het bestek van dit document, maar worden bijgehouden in de operationele discipline van het project.

---

5. Ontwerpprincipes

5.1 Tenant isolatie als basis, niet als functie

De eerste prioriteit van de architectuur is dat tenantisolatie de fundamentele basis is. Elke databasequery wordt gefilterd op `tenantId`. Het filter wordt afgedwongen door een databaseplugin die draait tegen een `AsyncLocalStorage-verzoekcontext`; queries buiten de verzoekcontext (geplande taken, batchjobs) moeten zich expliciet afmelden en documenteren waarom. Er is geen platformbeheerdersrol met toegang tot inhoud van andere tenants; een platformbeheerder kan tenants aanmaken en beheren (infrastructuurbeheer), maar kan geen tenant-inhoud lezen. Dit is geen configuratieoptie — het wordt afgedwongen in de code, en elke poging tot toegang tot andere tenants wordt behandeld als een beveiligingslek.

De discipline is duurzaam. Een enkel intern geheugenrecord, gemarkeerd als “nooit inkorten”, verwoordt het principe: *“Tenantisolatie IS het product. Zonder dit is er geen*

soevereiniteit.” Dit is een interne technische regel, afgedwongen door codereview en door geautomatiseerde tests die mislukken als een query wordt opgebouwd zonder een tenantfilter.

5.2 Metadata van soevereine records als uniform schema

Elk inhoudsmodel dat deel uitmaakt van het soevereiniteitsverhaal bevat hetzelfde metadatablok, toegepast via een databaseplugin:

```
metadata: {
  origin: {
    author_did, kaitiaki, collective_id,
 tikanga, 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
  },
  encryptie: { sleutel-id, algoritme },
  proof_chain: [{ boundary_crossed, policy_evaluated_by, decision,
                  caveats_added, timestamp, algorithm,
                  signature, signer_did }],
  verification_cache: { verified_at, chain_hash_at_verify,
                        algorithms_verified, re_verify_after }
}
```

Het schema is identiek voor alle door de tenant gegenereerde inhoudsmodellen — Story, Poll, Event, Media, Album, Comment, ChatMessage, Deliberation, Correspondence, NewsPost, Resource, CommunityResource, ResourceBooking — en voor een uitgebreide reeks ingebedde oppervlakken (subdocumentdekking van EventMenu, Edition en dergelijke). Het aanmaakpad van elk model leidt de oorsprong af via een gedeelde helper; de pre-save hook van de plug-in berekent de provenance-hash en ondertekent de aanmaakvermelding; de post-save hook slaat de verificatiestatus op in de cache; leesbewerkingen voorzien elk record van een verificatieveld dat de versheid van de cache aan consumenten toont. De uniformiteit is het punt: er is geen op maat gemaakte soevereiniteitsimplementatie per model, en dus geen risico op soevereiniteitsregressie per model.

5.3 Cryptografische herkomst met algoritmische flexibiliteit

Provenance wordt berekend als SHA-256 over een canonieke JSON-serialisatie van de verplichte en optionele velden van de oorsprong. Het algoritme wordt genoemd in `provenance_algorithm`, zodat een toekomstige migratie naar een andere cryptografische primitief (bijv. NIST post-kwantumkandidaten) geen schemaverandering vereist — alleen een nieuw entry-point in dezelfde canonieke

vorm. Handtekeningbewerkingen op proof-chain-vermeldingen bevatten op dezelfde manier hun `algoritmeveld`; de crypto-flexibiliteitswrapper van het platform ondersteunt momenteel Ed25519 en is zo gestructureerd dat het extra algoritmen accepteert zonder dat er wijzigingen in de aanroeplocatie nodig zijn.

Dit is bewust gedaan. Records met een lange levensduur overleven de cryptografische primitieven waarmee ze zijn ondertekend. Een architectuur die haar primitief hardcodeert kan geen aanspraak op soevereiniteit waarmaken die langer duurt dan de levensduur van de primitief .

De geschatte horizon voor cryptografisch relevante kwantumcomputers (CRQC's) is 10–30 jaar. De NIST-normen voor post-kwantumhandtekeningen werden in augustus 2024 afgerond (FIPS 204 ML-DSA, op roosters gebaseerd; FIPS 205 SLH-DSA, op hashes gebaseerd), waarmee het migratietraject volgens de normen werd vastgesteld; de hierboven beschreven algoritme-agility-wrapper maakt de overgang mogelijk zonder wijzigingen per aanroeplocatie. Twee verdere eigenschappen begrenzen de vervalsingskosten per record onder CRQC-dreiging: een vervalst record moet consistent blijven bij N onafhankelijke verifiers die elk hun eigen ground-truth-records bezitten (de kosten voor gedistribueerde verificatie komen bovenop de cryptografische breekkosten); en de substraatmechanismen gespecificeerd in §7 (bilaterale federatie) en §8 (soevereine overdraagbaarheid) zijn niet afhankelijk van de integriteit van de handtekening per record. Aantasting van de cryptografische primitief heeft geen domino-effect op de andere substraatmechanismen.

5.4 Beleidsovererving met berekening van effectief beleid bij de leesgrens Beleid

Beleid is geen enkel veld; het is een hiërarchie. Elke tenant heeft een soevereine grondwet waarin de standaardinstellingen worden vastgelegd; elke subgroep kan deze overschrijven; `het metadata.policy-blok` van elk record kan verdere specificaties bevatten. Op het moment van lezen wordt een effectief beleid berekend voor het verzoekende lid aan de hand van de beleidsstack van het record. De Policy Inheritance Engine voert deze berekening uit; de poort wordt afgedwongen bij de routegrens via aanroepen per lijst en per detail.

De engine wordt op meerdere niveaus getest: unit-tests per regel, validatie van use-cases tegen live lokale databases, en een werkwijze waarbij tests aantonen dat de koppelingen werken in mock-omgevingen, maar use-cases bewijzen dat het ook in de praktijk werkt. Deze laatste werkwijze — die is ingevoerd na een incident waarbij een omvangrijke reeks unit-tests zonder fouten doorliep voor een functie die in de productieomgeving niet was gekoppeld — is vastgelegd in de werkwijze van het project.

Drie filteropties beperken de toegang tot specifieke toegangspatronen: origin-only beperkt het lezen tot de auteurs-ID's van het record; group-scope beperkt het lezen tot leden van de `collective_id-` subgroep van het record; de strikte modus van unknown-scope CLOSED op elke `share_within-waarde` die de poort niet herkent — diepgaande verdediging tegen verkeerd geconfigureerde tenant-samenstellingen of via federatie geïmporteerde records met scope-waarden buiten de door het platform herkende set.

5.5 Bilaterale federatie in productie

Federatie in de zin van dit document is de enge technische regeling van §2.4 en §4. De constituties van twee tenants zijn het eens over het afgebakende doel van de federatie; beide operators ondertekenen het federatiemanifest; de gegevensstroom is direct tussen de twee tenants; beide kunnen op elk moment herroepen. Het federatiemanifest zelf is een soeverein record — het bevat zijn eigen herkomst, zijn eigen beleid, zijn eigen bewijsketen en zijn eigen verificatiecache.

De federatie-infrastructuur wordt end-to-end in het platform geleverd: het overeenkomstenmodel, de overeenkomstservice, het routeoppervlak, een beheerders-UI, een auditlogpad en een uitgebreide negatieve-testmatrix die scope-gebonden leesbewerkingen, het blokkeren van schrijfbewerkingen tussen tenants, de volledigheid van auditlogs, citatiediscipline, caching/veroudering, randgevallen van gegevensstatussen, autorisatiegrenzen en naamruimteconflicten omvat. Live federatiekoppelingen tussen onafhankelijke tenants zijn in afwachting van de eerste multi-instance-implementatie; het bilaterale patroon is gebouwd, de implementaties nog niet. §7 beschrijft de implementatie in detail.

5.6 Door leden gestuurde soevereine overdraagbaarheid

Een lid dat zijn tenant wil verlaten — om te migreren naar een andere tenant die onder hetzelfde architecturale model opereert, om zijn materiaal naar een andere gemeenschap te brengen, of om te voldoen aan het recht op inzage uit artikel 15 van de AVG — kan dit doen via een canonieke export. De export bevat elk record waarin het lid de auteur, de kaitiaki of anderszins als betrokkene wordt genoemd; elk record draagt zijn bewijsketen mee; de ontvangende partij kan de keten verifiëren aan de hand van het gepubliceerde DID-document van de brontenant zonder een van beide operators te vertrouwen. Records waarvan het beleid export verbiedt (bijv. een bijdrage aan een beraadslaging onder voorwaarden van collectieve toestemming) worden in het exportmanifest vermeld als achtergehouden, met vermelding van de beleidsreden.

Dit is het architecturale kader van artikel 15 van de AVG: geen toegangspunt voor speciale doeleinden, maar dezelfde exportpijplijn die de architectuur gebruikt voor alle verplaatsingen van soevereine records, geïnstantieerd voor het geval van de betrokkene als lid. §8 beschrijft de implementatie, inclusief het opnamepad van de ontvangende tenant dat de migratielus sluit.

---

6. Architecturale implementatie

Dit hoofdstuk beschrijft de componenten die de ontwerpprincipes van §5 in code realiseren. Elk daarvan is in productie op beide infrastructuurlocaties (OVH Frankrijk onder EU-soevereiniteit; Catalyst Cloud onder Nieuw-Zeelandse soevereiniteit) en verifieerbaar vanuit de codebase en de actieve API-interface. Conform de IP-perimeterhouding (§13) beschrijft dit rapport architecturale componenten en hun interacties in plaats van bronpaden per bestand.

6.1 Cryptografische herkomstprimitief

De herkomstprimitief berekent SHA-256 over een canonieke JSON- serialisatie van de verplichte en optionele velden van de bron. Het ingangspunt produceert de hash; een verificator berekent deze opnieuw en vergelijkt deze met de opgeslagen hash. De algoritme-identificatie reist mee met het record. Een helper voor de canonieke vorm elimineert van de hydratatiemodus afhankelijke enumeratie — een foutmodus die aan het licht kwam tijdens de validatie van use-cases, waarbij een serialiser die de enumerable-eigenschappen van een ORM-subdocument doorliep hashes produceerde die verschilden tussen hydratatiemodi, terwijl een omvangrijke suite van unit-tests op payloads met gewone objecten zonder problemen doorliep. De oplossing was een enkele normalisatiestap; de discipline die dit aan het licht bracht (validatie van use-cases tegen live databases, niet alleen gesimuleerde tests) maakt nu deel uit van de werkwijzen van het project.

6.2 Proof-chain-ondertekening bij aanmaken, bijwerken en verwijderen

Elke schrijfbewerking naar een record met een soeverein-tag voegt een ondertekende vermelding toe aan de proof-chain van het record. CREATE-vermeldingen worden ondertekend door de proof-signing-sleutel van de tenant (geleverd via de tenant-sleutelopslag, §6.6) en binden de vermelding aan de provenance-hash van het record. UPDATE-vermeldingen bij schrijfbewerkingen in documentmodus worden alleen uitgezonden wanneer soeverein-relevante paden zijn gewijzigd (met uitzondering van boekhoudvelden zoals `updatedAt`); de gewijzigde padenlijst wordt vastgelegd. UPDATE-vermeldingen in query-modus volgen dezelfde vorm, berekend op basis van het verschil tussen pre-image en post-image documenten op `updateOne`, `updateMany`, `findOneAndUpdate` en gerelateerde paden. DELETE-kruisingen worden afgehandeld door twee hook-lagen — een document-mode hook en een query-mode hook die single-, batch- en findAndDelete-varianten omvatten. Beide lagen produceren een Tombstone-record met de ondertekende verwijderingsvermelding als bewijs van de verwijdering; query-mode tombstones zijn waarneembaar te onderscheiden van document-mode tombstones via het `policy_evaluated_by-veld`. Een afzonderlijke component breidt dit uit naar het governance-wachtrijmodel, waardoor wordt gewaarborgd dat ook governance-interne verwijderingen een ondertekend cryptografisch spoor achterlaten.

6.3 Verificatie caching en read-path-integratie

Verificatie van de bewijsketen vindt plaats bij opname en wordt gecachet in het verification-cache-blok van het record: het tijdstip van de laatste verificatie, de SHA-256 van de gecanoniseerde bewijsketen op dat moment, de geverifieerde algoritmen en de volgende deadline voor herverificatie (standaard 90 dagen; door de tenant configureerbaar via de constitution). De verifier biedt drie toegangspunten: een verify-and-cache op het moment van opname, een synchrone cachecontrole op het moment van lezen en een geplande batch-sweep.

De bedrading is uniform. Een pre-save hook berekent de herkomst en ondertekent de aanmaakvermelding. Een post-save hook activeert 'verify-and-cache' na elke schrijfbewerking, gedempte door een in-flight sleutel om stormcondities te

voorkomen. Een geplande taak draait dagelijks op de door de tenant gegenereerde Een geplande taak wordt dagelijks uitgevoerd op de door de tenant gegenereerde contentmodellen, waarbij verlopen cache-items in batches worden verwerkt. De post-save-hook wordt geactiveerd bij aanmaken en bij soevereine updates; een padlijstfilter sluit boekhoudkundige paden uit, zodat de eigen schrijfbewerkingen van de verifier de hook niet op zichzelf laten herhalen; opslag die alleen voor boekhouding is bedoeld, slaat de verifier over en beperkt de kosten van herverificatie tot echte soevereine wijzigingen.

Het leespad maakt het geheel compleet. Elk API GET-antwoord op een soevereingetagd record bevat een verificatieveld: compact `{valid, reason}` bij lijstantwoorden, uitgebreide extra's (verified-at, re-verify-after, algorithms-verified) bij detailantwoorden. De implementatie is uniform: één enkele decorator-helper wordt aangeroepen vanuit de lean- en aggregate-paden van elke route.

6.4 Beleids-overervingsengine en handhaving op groepsniveau

De Policy Inheritance Engine leest uit de tenant-constitutie, de subgroep-lidmaatschappen van het verzoekende lid, het beleidsblok van het record en de gevraagde bewerking (lezen/schrijven/exporteren/verwijderen). Het retourneert een effectief beleid met expliciete redenen voor schending wanneer een verzoek mislukt. Drie filteropties versmallen de toegang volgens §5.4.

Handhaving op groepsniveau is afhankelijk van records met een geldige `collective_id`. Een helper valideert een door de aanroeper verstrekte subgroep-identificatie aan de hand van drie beperkingen (formaat, tenant-bereik, kijkerslidmaatschap) en retourneert een atomaire context — atomair omdat `collective_id` zonder `share_within: ['group']` puur decoratief is (de poort zou niet handhaven). Acht content-create paden (Poll, Event, Story, Album, Deliberation, ChatMessage, Carpool, Resource) accepteren de subgroep-identificatie uit de verzoektekst en sturen deze door via de helper. Achterwaartse compatibiliteit blijft behouden: aanroepers die het veld weglaten, maken records op tenant-niveau zoals voorheen. UI-kiezers per formulier tonen de subgroepselectie op het niveau van het aanmaakformulier over de acht oppervlakken.

De strikte modus voor onbekende scopes dicht een fail-open-lek dat aanwezig was in eerdere iteraties. Een platformbrede set van erkende scope-waarden definieert de woordenschat; elke waarde buiten deze set wordt nu geweigerd met een benoemde reden, tenzij een erkende scope in dezelfde set al toegang verleent. Dit is het standpunt van het project — *wees eerlijk over wat niet kan worden geverifieerd; verzin er geen toestemming voor* — toegepast op de read-path-gate.

6.5 Soevereine grondwet editor

De soevereine grondwet van een tenant kan door de tenantbeheerder worden bewerkt via een speciale route en frontend. De editor toont de constitutionele standaardinstellingen (standaardresolutiemodus, standaardexportmodus, standaardveronderstelde autoriteit, versleutelingsmodel), een categorietabel die de canonieke inhoudsmodellen vastlegt en door de tenant gedefinieerde aangepaste categorieën toestaat, en

meertalige ondersteuning voor Engels, Duits, Frans, Nederlands en Te Reo Māori. De vertalingen in het Te Reo Māori zijn gemaakt met behulp van de vertaaltools van het project (DeepL, dat Te Reo Māorionder steunt onder de taalcode `MI` — een feit dat regelmatig verkeerd wordt aangenomen door externe commentatoren en binnen het project zelf is gecorrigeerd) en steekproefsgewijs gecontroleerd op de juiste betekenis.

Een constitutioneel overgangsvenster houdt in dat tenants die hun constitutie bewerken een banner te zien krijgen waarin staat dat de wijziging pas na de overgang bindend wordt; dit is de constitutionele voorwaarde die het verschil maakt tussen een conceptconstitutie en een bindende. Een afzonderlijke gate (de sovereign-constitution gate) dwingt 403 af voor tenants die na de overgangsdatum zijn aangemaakt en die de vereiste soevereine secties missen, met ingebouwde opschortingsimmuniteit voor aangewezen platform-infrastructuur- tenants.

6.6 Sleutelopslag van de tenant

De versleutelings- en ondertekeningssleutels van elke tenant bevinden zich in een sleutelopslagplaats op tenantniveau met bewerkingen voor het genereren, ophalen, roteren en vernietigen ervan. Sleutels worden aangeduid door identificatiecodes die zijn opgeslagen in het versleutelingsblok van elk record. Cryptografische verwijdering van een record — beleidsgebonden door de vlag `delete_must_be_cryptographic` — verloopt door de versleutelingssleutel per record in de sleutelopslag van de tenant te vernietigen, waardoor de gecodeerde tekst van het record onherstelbaar wordt vanuit de persistente toestand.

6.7 Gedecentraliseerde publicatie van identificatiecodes

Gedecentraliseerde identificatiecodes van tenants en leden volgen de W3C DID-specificatie [11] en worden gepubliceerd onder het domein van de tenant (`/.well-known/did.json` voor het tenant-DID-document; `/.well-known/did/members/${slug}/did.json` optioneel voor lid-DID's). DID-documenten bevatten de verificatiemethoden van de tenant die worden gebruikt om proof-chain-vermeldingen te ondertekenen; een externe verificateur die in het bezit is van het DID-document van de tenant kan elke ondertekende vermelding in een record verifiëren, inclusief vermeldingen op records die onder §8 naar een andere tenant zijn geëxporteerd.

6.8 Governance-wachtrij

Het governance-wachtrijmodel legt gevallen vast die een beslissing van de tenant-arbiter vereisen: beleidsschendingen, verzoeken tot conflictoplossing, door leden geïnitieerde verwijderingsverzoeken die goedkeuring van het bestuur vereisen. Levenscyclusstatussen — aangemaakt → in behandeling → beslist → uitgevoerd (of afgewezen) — zijn overgangsgebonden; elke beslissing en elke uitvoering laat ondertekende spoorvermeldingen achter die de tenant kan reconstrueren vanuit zijn eigen database. Handhaving van deadlines wordt automatisch uitgevoerd volgens de constitutionele standaardresolutie van de tenant wanneer een vermelding de respijtperiode overschrijdt .

6.9 Exportwrapper met overlay voor zichtbaarheid voor niet-beheerders en symmetrische auditlogging

Elke export van soevereine records gaat door een wrapper die aan drie voorwaarden voldoet: elk record bevat herkomstinformatie; elk record behoort toe aan de aanvragende tenant; de volledige modus vereist de rol van tenant-beheerder. Hash- en aggregatiemodi zijn nu beschikbaar voor gewone leden via een zichtbaarheidsoverlay die records filtert naar de leeshorizon van de aanroeper voordat de projectie wordt geproduceerd — eigenaar-bypass; regels per zichtbaarheidsniveau; fail-secure bij fouten bij het voorladen van subgroepen. Overtredingen schrijven een governance-auditlog-vermelding met een toelichting. Succesvolle exporten schrijven ook een auditvermelding met metadata over de vastleggingsmodus (volledig/hash/geaggregeerd), het aantal records voor en na het filteren, een uitsplitsing per model en de identiteit van de aanroeper. Elke export — succesvol of in strijd met de regels — kan worden gereconstrueerd uit het auditlogboek; geen enkele export is stil.

6.10 Uniforme migratie van soevereine records binnen de door tenants gegenereerde inhoudsmodellen

Het metadatablok voor soevereine records wordt uniform toegepast in de door tenants gegenereerde inhoudsmodellen. De migratie was waar mogelijk 'lazy' (records krijgen de metadata bij de eerste schrijfbewerking onder het nieuwe schema) en waar nodig 'eager' (een eenmalig script vulde de herkomstgegevens in voor de bestaande recordvoorraad). Hetzelfde metadatablok strekt zich uit tot ingebedde subdocumentoppervlakken (EventMenu, Edition en dergelijke) onder een uniforme plugin-uitbreiding. De verificatiecache wordt gevuld voor de operationele tenant-set op beide productiesites; het kleine restant van legacy-records zonder herkomst-hash wordt gemarkeerdals `niet-verifieerbaar` in plaats van `geldig` — de architecturale keuze is om datgene wat niet kan worden geverifieerd aan de oppervlakte te brengen in plaats van er een cache voor te synthetiseren.

6.11 Afstemming van beleid voor workers en WebSockets De

De asynchrone workerlaag past het constitutionele beleid van de tenant toe op de records die deze aanmaakt. De twee create-path-workers binnen het toepassingsgebied (verwerking van e-mail naar inhoud; het scannen van documenten) roepen een gedeelde helper aan die een beleidscontext samenstelt uit de metadata van de oorspronkelijke taak (tenant-identificatie; identificatie van het oorspronkelijke lid; identificatie van de oorspronkelijke subgroep, indien van toepassing) en stelt `metadata.origin` en `metadata.policy` in op het record op het moment van aanmaken. Workers die bestaande soevereine records bijwerken (OCR-verrijking van geüploade bijdragen; mediaverbetering; verhaal extractie; spraakvalidatie) behouden het beleid dat is ingesteld op het moment van aanmaken en hebben de helper niet nodig. Workers die geen soevereine inhoud produceren (coördinatie door de orchestrator; scannen van wachtrijen; transcriptiepijplijnen die operationele wachtrijrecords wijzigen) werden binnen het toepassingsgebied gecontroleerd en er werd bevestigd dat ze de helper niet nodig hebben. Het WebSocket- oppervlak is

gekoppeld aan dezelfde berekening van het effectieve beleid via een broadcastfilter per ontvanger; voordat een chatbericht een ontvangersocket bereikt, wordt het zichtbaarheidspredikaat voor die socket geëvalueerd, en wordt het bericht weggelaten als de zichtbaarheidscontrole mislukt. Federatie- broadcasts gaan ongewijzigd door — de zichtbaarheid van de federatie wordt bepaald op het niveau van de federatieservice, niet op het niveau van de broadcast.

6.12 Proof-chain compaction primitive

Een primitief voor het comprimeren van bewijsketens vervangt een aaneengesloten subbereik van de bewijsketen van een record door een enkele ondertekende samenvattingsvermelding waarvan de payload de SHA-256 is van de canonieke JSON van de vervangen subketen. Verificatie van een gecomprimeerd item kent twee modi: een standaard goedkope modus behandelt het gecomprimeerde item als een enkele ondertekende stap, verankerd door de samenvattingshash; een volledige modus haalt de gearchiveerde subketen van vóór de compressie op en verifieert item voor item. De primitieve is opt-in per tenant-constitutie; standaard is deze uitgeschakeld. Toepassing op live tenant-bewijsketens gebeurt op het tempo van de operator.

6.13 Tombstone-retrofit

Een tombstone-retrofit-primitief ondertekent reeds bestaande tombstones in platte tekst van vóór de introductie van proof-chain-ondertekening, zodat het audittraject uniform is in de hele geschiedenis van de tenant. De retrofit werkt per tenant, idempotent en hervatbaar, en voegt een ondertekend item toe naast de originele velden in platte tekst zonder deze te wissen. De primitief wordt door de operator bepaald; er zijn nog geen tombstones van productietennants retrofit.

6.14 Framework consultatie als audit trail

Elke architecturale beslissing in de ontwikkeling van het platform wordt voorafgegaan door een frameworkconsultatie: een gedocumenteerd beslissingsverslag waarin de geraadpleegde diensten, de lijst met voorwaarden per dienst en het oordeel worden vermeld. Consultaties worden vastgelegd in lokale, EU-soevereine en Nieuw-Zeelandse soevereine productiedatabases. De registratie wordt geautomatiseerd door scripts per beslissing; de documentvorm is een markdown-bestand per beslissing in de `map docs/framework-consultations/`. De discipline van het registreren — drie invoegpunten per consultatie, zodat het verlies van één enkele host de auditpositie niet in gevaar brengt — is de bijdrage; de waarde is reproduceerbaarheid en controleerbaarheid, niet het aantal records.

Dit is geen virtue-signalling. De consultatie is het mechanisme van het project om architecturale beslissingen te koppelen aan waarneembare artefacten: een toekomstige lezer kan vragen, *welke voorwaarden werden door de read-path-integratie aangepakt?*, en het antwoord staat in de database. Het werkdocument vanTractatus [1] documenteert het patroon vanuit het framework; dit document documenteert een voorbeeld ervan vanuit het platform, waarbij het consultatieledger deel uitmaakt van het evaluatieoppervlak (§12).

7. Bilaterale federatie in productie

Het bilaterale federatiepatroon is end-to-end opgebouwd, met een substantieel verificatieoppervlak; live federatiekoppelingen tussen onafhankelijke tenantimplementaties staan nog in de wacht. De architectuur is klaar voor de eerste multi-instance-implementatie; de implementaties zijn nog niet gerealiseerd.

7.1 Het federatiemanifest

Een federatie tussen twee soevereine tenants wordt gematerialiseerd als een federatieovereenkomst die door beide tenants is ondertekend. De overeenkomst specificeert het afgebakende doel (carpool-ride-matching, aankondiging van gedeelde evenementen, gezamenlijke beraadslaging, kaupapa co-beheer, domeinoverschrijdende verwijzing naar leerplannen), de vorm van de gegevensstroom (welke velden in welke richting, welke transformatie, welke bewaring aan elke kant), de beleidsafhandeling tussen tenants (welke grondwet is van toepassing op records die onder de federatie zijn opgesteld; hoe beleidsconflicten worden opgelost), de intrekkingsprocedure (elke partij kan eenzijdig intrekken; intrekking is een ondertekend record; verspreiding is onmiddellijk), en de auditbewaring (elke tenant bewaart een ondertekend exemplaar van elke interactie tussen tenants).

Het manifest is zelf een soeverein record. Een federatie kan niet worden geactiveerd zonder geverifieerde handtekeningen van beide partijen tegen hun respectievelijke DID-documenten. Bijlage C beschrijft de schemavorm op architecturaal-componentniveau; specifieke details over de implementatie van velden worden achtergehouden volgens het IP-perimeterbeleid (§13).

7.2 Beheerders-UI en auditlogboek Een

Een tenantbeheerder beheert federatieovereenkomsten via een speciale beheerders-UI die de levenscyclus van de federatie weergeeft (voorgesteld → geaccepteerd → actief → ingetrokken) en het auditlogboek weergeeft. Elke grensoverschrijdende gebeurtenis — een federatievoorstel, een aanvaarding, een query die via de federatie wordt gerouteerd, een intrekking — laat een ondertekende vermelding achter in het auditlogboek van de federatie. Het auditlogboek kan aan beide kanten onafhankelijk worden gereconstrueerd; geen van beide tenants vertrouwt op de administratie van de ander voor zijn eigen auditpositie.

7.3 Negatieve-testmatrix

Een negatieve-testmatrix (onder continue-integratiedekking) bevestigt de invarianten van het federatieoppervlak. Er zijn twaalf categorieën opgezet: scope-gebonden leesbewerkingen (inclusief een statische controle dat er geen verboden collectieverwijzing voorkomt in de federatieservicecode), schrijfblokkering tussen tenants, volledigheid van het auditlogboek, citeringsdiscipline, caching-/verouderingsgedrag, randgevallen van gegevensstatussen (ontbrekende velden; onderscheid tussen null en afwezig),

handhaving van autorisatiegrenzen en oplossing van naamruimteconflicten in fase 3. Een subset van de matrix wordt doorlopen door een live multi-tenant validator die de volledige HTTP-stack test tegen een actieve implementatie; de rest wordt uitgevoerd tegen een fixture op serviceniveau of als statische code-grep-beweringen.

De meest belastende test in de matrix is een statische bewering: het federatieservicebestand wordt als tekst gelezen, opmerkingen worden verwijderd en verboden collectienamen worden vergeleken met de uitvoerbare code. De bewering is gecodeerd als een test per CI, niet als een eenmalige pre-commit-controle; elke toekomstige uitbreiding van het leesoppervlak van de federatie die een verboden collectiereferentie introduceert, zorgt ervoor dat de bewering op CI-moment faalt.

7.4 Status van live implementatie

Live federatiekoppelingen tussen onafhankelijke tenants wachten op de eerste multi-instance-implementatie. De carpoolfederatie — een klasse van federaties die een reeks gemeenschappen verbindt voor uitsluitend Koha-gerichte ritbemiddeling — is de oorspronkelijke beoogde multi-instance-implementatie. Een carpool-tenant wordt gebouwd op NZ-soevereine infrastructuur (Catalyst Cloud); de multi-instance federatie wordt geactiveerd zodra ten minste twee carpool-tenants operationeel zijn. **Gemeenschappen of organisaties die de multi-instance carpool-implementatie verkennen als een alternatief voor soevereine infrastructuur — beoefenaars van gemeenschapsvervoer, onderzoekers op het gebied van vervoersgelijkheid , programma's voor veerkracht op het platteland, universitaire duurzaamheids- of vervoersgroepen — worden uitgenodigd om contact op te nemen met de corresponderende auteur met betrekking tot deelname aan de pilot.**Iwi-naar-iwi-federatie- implementaties — waarbij de ene iwi specifiek kaupapa-materiaal deelt met een andere, via een ondertekend manifest, met behoud van volledige controle over intrekking — worden infrastructureel ondersteund maar zijn operator-geleid; op het moment van dit concept is er nog geen actieveiwi-naar-iwi- federatie geactiveerd.

De formulering van bilaterale federatie in §5.5 is daarom een *architectonische toezegging met geleverde infrastructuur en een verificatieoppervlak*, niet een *geïmplementeerd netwerk van actieve federaties*. De architecturale eigenschap die hier op het spel staat — dat twee gemeenschappen, op door hen gespecificeerde voorwaarden, kunnen instemmen met een specifieke, afgebakende interactie, en alleen dat — is precies wat de drie artikelen van Te Tiriti impliceren voor digitale infrastructuur: tribale soevereiniteit over taonga wordt geëerbiedigd omdat elke iwi volledige autoriteit behoudt binnen zijn eigen tenant, en federatie tast die autoriteit niet aan — het staat een specifieke, afgebakende interactie toe binnen het kader van de architectuur.

---

8. Soevereine overdraagbaarheid — DSR-integratie

De zesde ontwerpverplichting van de architectuur (§5.6) is dat een lid een eersteklas betrokkene is. Een lid dat zijn tenant wil verlaten — om te migreren naar een andere

tenant binnen hetzelfde architecturale model, om zijn materiaal mee te nemen naar een andere gemeenschap, of om te voldoen aan een recht van de betrokkene onder de AVG — kan dit doen via een canonieke export.

8.1 De canonieke exportbundel Een

Een door een lid geïnitieerde canonieke export bevat elk record waarin het lid de auteur, de kaitiaki of anderszins als betrokkene wordt genoemd. De export is een gepagineerde bundel van de door de tenant gegenereerde, soeverein-getagde inhoudsmodellen, inclusief ingebedde oppervlakken waar van toepassing. Elk record in de bundel bevat zijn volledige bewijsketen, zijn volledige beleidsblok en zijn herkomst-hash. Het manifest van de bundel is zelf ondertekend door de brontehuurder; een externe verificateur die in het bezit is van het DID-document van de brontehuurder kan elke ondertekende vermelding in de bundel verifiëren zonder een van beide operators te vertrouwen. De bundel wordt weergegeven in JSON-, CSV- of PDF-formaat, afhankelijk van het verzoekformaat; de onderliggende canonieke inhoud is identiek in alle weergaven.

8.2 Beleidsconforme export en manifest met lijst van achtergehouden items

De exportwrapper handhaaft het beleid. Records waarvan het beleid export verbiedt (bijv. een beraadslaging bijgedragen onder collectieve-toestemmingsvoorwaarden; een mediabestand dat onderworpen is aan een tikanga deelbeperking) worden in het exportmanifest vermeld als achtergehouden, met vermelding van de beleidsreden. Het lid ontvangt zowel de bundel als de lijst met achtergehouden items; de lijst met achtergehouden items is zelf ondertekend, zodat het lid een verifieerbaar bewijsstuk heeft dat aantoont wat is uitgesloten en waarom. De discipline is volledige openbaarmaking van wat wordt achtergehouden en waarom: een poging om een recht van de betrokkene als voorwendsel te gebruiken voor toegang tot materiaal waar het lid geen legitiem recht op heeft, wordt tegengehouden door de beleidsbarrière, en het antwoord zelf is controleerbaar.

Het mechanisme van de lijst met achtergehouden gegevens is het architectonische antwoord op een spanningsveld dat toezichthouders al jaren signaleren: het recht op inzage in artikel 15 wordt begrensd door de rechten van andere identificeerbare personen (artikel 15, lid 4) en door andere gronden voor legitieme verwerking. Een standaardimplementatie kan ofwel alles teruggeven (waardoor de rechten van andere partijen worden geschonden) ofwel minder dan gevraagd (zonder de grond voor uitsluiting uit te leggen). Het uitgangspunt van de architectuur is dat elk uitgesloten record wordt benoemd, de beleidsreden wordt aangehaald en het manifest dat beide onderdelen bindt, verifieerbaar is.

8.3 Opname door ontvangende tenant (migratie tussen tenants)

Een lid kan zijn canonieke exportbundel meenemen naar een andere tenant die volgens hetzelfde architectuurmodel werkt. Het importpad van de ontvangende tenant verifieert de bewijsketen van elk record aan de hand van het DID-document van de brontetenant, accepteert de records (voor zover de statuten van de ontvangende

tenant dit toestaan) en zet de bewijsketen voort — de ontvangende tenant ondertekent een `ingest_via_migration-vermelding` op elk record, waarbij de brontetenant en de hash van het bundelmanifest worden vermeld. De identiteit van het lid wordt vastgesteld aan de hand van zijn tenantoverschrijdende DID; de migratie wordt aan beide kanten geregistreerd als een normale soevereine-recordgebeurtenis. Een grondwettelijke acceptatiecontrole door de ontvangende tenant is integraal, niet optioneel: records waarvan het beleid van de brontetenant onverenigbaar is met de standaardinstellingen van de ontvangende tenant (bijv. een strikter privacybeleid dat een soepeler afzenderbeleid weigert) worden vermeld als AFGEWEZEN met de beleidsreden. Het ontvangstbewijs van de gemigreerde bundel wordt ondertekend door de ontvangende tenant en teruggestuurd naar het lid, wat een verifieerbare afsluiting van de migratie biedt.

De huidige implementatie van het opnamepad van de ontvangende tenant omvat fasen A–F: bron-DID-resolutie, bundelverificatie, grondwettelijke acceptatiecontrole, opname met voortzetting van de proof-chain, ondertekening van het ontvangstbewijs en end-to-end integratietestscenario's in overleg met het framework. Identiteitsafstemming in de v1-implementatie is zo geconfigureerd dat auto-onboarding standaard wordt geweigerd — een migrerend lid moet al lid zijn van de ontvangende tenant, of de beheerder van de ontvangende tenant moet de aanmaak van het lidmaatschap handmatig goedkeuren voordat de bundel wordt ingevoerd. Dit is een bewuste conservatieve keuze: auto-onboarding via cross-tenant DID heeft een beveiligingsoppervlak dat een eigen ontwerpronde rechtvaardigt, en de v1 implementatie stelt dit uit.

8.4 GDPR-artikelen 15, 16, 17, 18, 20, 21

Het DSR-eindpunt implementeert alle zes de rechten van de betrokkene volgens de AVG via dezelfde exportpijplijn, met recht-specifiek gedrag waar dat nodig is:

- **Artikel 15 (Recht op inzage):** de canonieke export, zoals beschreven in §8.1–§8.2.
- **Artikel 16 (Recht op rectificatie):** leden kunnen om correctie verzoeken; het verzoek is aan beleid onderworpen; geaccepteerde correcties laten een ondertekende proof-chain-vermelding achter.
- **Artikel 17 (Recht op verwijdering):** gegevens die uitsluitend door het lid zijn aangemaakt, en waarbij geen andere rechten in het geding zijn, kunnen op verzoek cryptografisch worden verwijderd — de versleutelingssleutel per gegevensrecord wordt vernietigd in de sleutelopslag van de tenant; de versleutelde tekst wordt onherstelbaar; een ondertekende ‘tombstone’ registreert de verwijdering. Records waarbij andere partijen betrokken zijn (een opmerking op het verhaal van een ander lid; een bijdrage aan een overleg met meerdere auteurs) volgen de constitutionele standaard voor verwijdering met collectieve toestemming — de governance-wachtrij van de tenant ontvangt het verzoek, de betrokken partijen worden geraadpleegd volgens het proces van de tenant, en het resulterende besluit wordt uitgevoerd met een volledig audittraject.
- **Artikel 18 (Recht op beperking):** beperking wordt geïmplementeerd als een beleidsoverschrijving die verwerking verhindert terwijl het verzoek in

behandeling is; de overschrijving is zelf een soevereine-record gebeurtenis.

- **Artikel 20 (Recht op gegevensoverdraagbaarheid):** de canonieke bundel van §8.1, met het opnamepad van de ontvangende huurder van §8.3 als architectonische voltooiing.
- **Artikel 21 (Recht op bezwaar):** bezwaar wordt vastgelegd in het relevante record en verspreidt zich via de beleidsgate als een verwerkingsveto per record.

De reactietermijn van 30 dagen uit artikel 15 wordt afgedwongen door een auditlog-timer; gemiste reacties activeren een waarschuwing in de governance-wachtrij van de tenant.

8.5 De spanning met uitzonderingen van artikel 17

De architecturale invulling van de spanning rond het recht op verwijdering tussen artikel 17 en de uitzonderingen van artikel 17, lid 3 (vrijheid van meningsuiting; rechtsvorderingen) houdt niet in dat de spanning niet bestaat; de spanning is reëel. De architectuur kadert de oplossing expliciet in, in de constitutie van de tenant, met beleidsgestuurde implementatie en met een volledig audittraject. Een verzoek tot verwijdering van een lid wordt gehonoreerd voor zover de constitutionele resolutie dit toestaat; wanneer voorwaarden voor collectieve toestemming een meerpartijenproces vereisen, wordt het proces geregistreerd en wordt de daaruit voortvloeiende beslissing (verwijderen, redigeren, bewaren) ondertekend. Een externe auditor die het auditlogboek leest, kan precies reconstrueren welke uitzondering van artikel 17 werd ingeroepen, door wie, op welk document en met welk resultaat.

---

9. UI voor stakeholdergovernance

De governance-UI toont de constitutionele houding van het platform, de communicatiediscipline, de beslissingsgeschiedenis, het raadplegingsregister, het dialoogplatform en het beoordelingsplatform voor belanghebbenden. Het is een platform gericht op belanghebbenden, dat bewust leesbaar is gehouden voor parochiepenningmeesters en gemeenschapsoudsten in plaats van alleen voor ingenieurs. De UI bevindt zich op een aangewezen subdomein van de operations-hub-tenant en wordt via een uniform patroon gerepliceerd naar elk tenant-subdomein. Fasen 1 tot en met 7 zijn op de datum van dit document geleverd; Fase 6 (participatieve dialoog) en Fase 7 (generalisatie over producttypes heen) breiden het platform uit van alleen-lezen beoordeling naar participatief bestuur.

Twee patronen van stakeholderbetrokkenheid lopen door de interface. Het eerste is **uitnodiging**: een tenantbeheerder verstuurt een ondertekende uitnodiging voor een stakeholder waarin de uitgenodigde partij, de voor hen geopende interfaces en de vervaldatum van de uitnodiging worden vermeld; de stakeholder accepteert via een eenmalige URL; de resulterende sessie heeft dezelfde beleidsbeveiliging als een ledensessie, waarbij de leeshorizon beperkt is tot de uitgenodigde interfaces. De tweede is **een verzoek**: wanneer een belanghebbende toegang zoekt zonder voorafgaande uitnodiging, stuurt het platform het verzoek door naar de per

tenant geldende procedure zoals gedefinieerd in de grondwet van die tenant. De architecturale basiselementen — het versturen van een uitnodiging, het acceptatietoken, het ondertekende audittraject — zijn uniform voor alle tenants en worden beschreven in de onderstaande gefaseerde subparagrafen; de door de belanghebbende geïnitieerde verzoekprocedure wordt per Village in de grondwet gedefinieerd en wordt in dit document niet gespecificeerd. Referentiestatuten die door het platform worden verstrekt, zijn gedocumenteerd in de Statuutviewer (§9.1), maar zijn niet normatief.

9.1 Statutenviewer (Fase 1)

De Constitution Viewer geeft de stabiel verankerde, op belanghebbenden gerichte aggregatie van de drie primaire bronnen weer (de harde regels van het project, de nooit-afgekorte geheugenitems en de Layer 1 universele platformprincipes). De weergave is een markdown-page-loader patroon: geen API-route, geen dynamische opvraging; de viewer is een statisch HTML- bestand dat de markdown via HTTPS laadt en weergeeft. Dit patroon is opzettelijk: de viewer is het eenvoudigste mogelijke artefact, controleerbaar door elke reviewer die HTML en markdown kan lezen.

9.2 Comms Constitution-viewer (Fase 2)

De Comms Constitution-viewer volgt hetzelfde patroon en toont het communicatiereglement voor operators (kanaalstapel, cadans, weigering regels, regels voor concepten die nooit worden verzonden). De huidige gepubliceerde versie sluit de door operators ingevoerde items af onder het door de operator gedelegeerde beste oordeel; volgende herzieningen wachten op goedkeuring door de operator.

9.3 Beslissingslogboek-viewer (Fase 2)

De Decision-log viewer geeft een samengestelde index weer van belangrijke beslissingen gedurende de ontwikkeling van de architectuur (architecturale primitieven, leveranciershouding, privacy- en inhoudsregels, procesdiscipline, training en AI). Zowel de Constitution viewer als de Comms Constitution viewer linken in hun Companions-secties naar de Decision-log viewer. De volledige, voor belanghebbenden leesbare boog — Constitution → Comms Constitution → Beslissingslogboek — is doorzoekbaar op elk subdomein van de tenant.

9.4 Framework consultatieviewer (Fase 3)

De Framework-consultatieviewer toont het consultatielogboek via een voor belanghebbenden leesbare HTML-interface. De viewer presenteert een geaggregeerde index op documentreferentie (één rij per architectonische beslissing, met geraadpleegde diensten, voorwaarden, uitspraken en datums) en een detailweergave per beslissing die de volledige lijst met voorwaarden per dienst en het spoor van uitspraken toont. De viewer is alleen-lezen; het onderliggende register wordt geschreven door de geautomatiseerde consultatie-opnamescripts van het platform; de stakeholder leest maar schrijft niet.

9.5 Toegang via gasttoken voor belanghebbenden (Fase 4)

Een stakeholder-specifieke gastsessie verleent alleen-lezen toegang tot de governance-UI zonder dat volledige registratie als tenant-lid vereist is. Een platformbeheerder verstuurt een uitnodiging aan de stakeholder; de uitnodiging is een ondertekend record waarin de stakeholder, de uitgenodigde oppervlakken en de vervaldatum van de uitnodiging worden vermeld; de stakeholder accepteert via een eenmalige URL; de resulterende sessie heeft dezelfde policy-gate-status als een lidsessie, maar met een leeshorizon die beperkt is tot de uitgenodigde oppervlakken.

De architecturale eigenschap is dat de beoordeling door belanghebbenden zelf een soevereine recordinteractie is: elke uitnodiging, elke aanvaarding, elke lezing wordt gelogd, ondertekend en is reconstrueerbaar vanuit het audittraject. Een financier of beleidsbeoordelaar die de governance-UI van het platform heeft beoordeeld, kan een verifieerbaar record produceren van wat hij heeft beoordeeld, wanneer en aan de hand van welke versie van het onderliggende materiaal.

9.6 Beoordelingsoppervlak voor belanghebbenden (Fase 5)

Een definitief beoordelingsoppervlak bundelt het materiaal van de governance-UI in een enkele doorbladerbare index voor gebruik door belanghebbenden: een vermelding van één pagina die elk artikel van de grondwet, elke vermelding in het besluitlogboek, elke regel van de communicatiegrondwet en elke recente raadpleging over het kader noemt, met diepe links naar elk daarvan. Het oppervlak is het natuurlijke eindpunt van een uitnodiging in fase 4; een belanghebbende die de uitnodiging accepteert, komt op het beoordelingsoppervlak terecht en kan van daaruit verder navigeren.

9.7 Participatieve dialoog (Fase 6)

Het dialoogoppervlak van fase 6 zet de alleen-lezen governance-UI om in een participatieve interface. Belanghebbenden kunnen commentaar geven op artikelen van de Grondwet, vermeldingen in het Beslissingslogboek en regels van de Comms-Grondwet; opmerkingen zijn zelf soevereine records, waarop dezelfde mechanismen voor herkomst, beleid, bewijsketen en verificatiecache worden toegepast. De situatietaal-laag van het platform beantwoordt vragen van belanghebbenden uit het samengestelde corpus dat de governance-UI zelf onderhoudt, waarbij het corpus dient als het citatieoppervlak. De bescherming tegen hallucinaties is gelaagd: een aangescherpte systeemprompt stuurt het taalmodel in de richting van standaardweigering voor vragen buiten het corpus, en een filter voor citatiediscipline wijst antwoorden af die geen bron uit het corpus vermelden.

9.8 Generalisatie over verschillende producttypes heen (Fase 7)

Fase 7 generaliseert het dialoogoppervlak van fase 6 over de producttypes van het platform. Elk producttype heeft zijn eigen dialoogcorpuspaden, woordenschat en citatiepatronen. Fase 7.A levert de generalisatie per producttype; Fase 7.B bouwt het gedeelde dialoogcorpus met universele patronen; Fase 7.C koppelt het inline weergaveoppervlak voor goedgekeurde opmerkingen over de mdsl-viewerpagina's

heen met dynamische ankers en een openbare widget-API; Fase 7.D is de federatie-interface voor de dialooglaag, die gebruikmaakt van dezelfde bilaterale federatie-infrastructuur zoals beschreven in §7 (de negatieve-testmatrix wordt gedeeld, niet afzonderlijk; de federatie van opmerkingen van belanghebbendenVillage is een specifieke toepassing van het algemene bilaterale patroon); Fase 7.E registreert de communicatieconstitutieregel en de grootboekregel die de acceptatie van de interface documenteert.

Het cumulatieve effect van de fasen 1–7 is een governance-oppervlak voor belanghebbenden dat leesbaar, controleerbaar, navigeerbaar, participatief, federatiebewust en uniform toegepast is over de producttypes van het platform — ten koste van een aanzienlijk verificatieoppervlak (waarbij de bilaterale federatie-negatieve-testmatrix de grootste afzonderlijke bijdrager is) en de disciplinaire overhead van het uitvoeren van de framework-consultatie-registratie op elke architecturale uitbreiding.

---

10. Praktijkvoorbeeld: domeinoverschrijdende naamgevingssoevereiniteit tussen twee gesitueerde taalmodules

Deze paragraaf illustreert het bilaterale-federatiepatroon met een praktijkvoorbeeld, aangeleverd door de corresponderende auteur uit zijn lopende curriculumontwerpwerk. Het voorbeeld betreft curriculumintegratie in een basisschoolomgeving, maar het architecturale patroon is algemeen toepasbaar op elk paar gemeenschappen waarvan de houdingen ten aanzien van gegevenssoevereiniteit elkaar kruisen op een specifiek punt van domeinoverschrijdende autoriteit. Een afzonderlijke uiteenzetting is beschikbaar in het carpool-dorpstype waarnaar in §11 wordt verwezen: carpool isoleert de federatieprimitief van het bredere, op leden gerichte oppervlak van andere dorpstypen en is het minimale geval waarin het federatiegedrag van het patroon afzonderlijk kan worden onderzocht. Het huidige praktijkvoorbeeld illustreert federatie tussen twee domeinen met verschillende gezaghebbende inhoud; de carpool-uiteenzetting illustreert federatie tussen twee instanties van hetzelfde dorpstype.

10.1 De configuratie

Beschouw twee gesitueerde taalmodules, die elk opereren als een soevereine tenant op het platform:

- **Een module met botanische kennis** voor een regionale flora — bijvoorbeeld een Flora of New South Wales-module, eigendom van een botanische instelling die verantwoordelijk is voor de gevalideerde taxonomie, wetenschappelijke namen, verspreiding, ecologische aantekeningen en kruisverwijzingen naar wetenschappelijke bronnen. De eigenaren van de module onderhouden de inhoud volgens een continu verbeteringsproces: nieuwe ontdekkingen worden gevalideerd en geïntegreerd; correcties worden uitgegeven onder ondertekende bevoegdheid; het corpus is de gezaghebbende bron voor botanische referentie binnen het toepassingsgebied van de module.

- **Een module voor taalrevitalisering** voor een inheemse taal in dezelfde regio — bijvoorbeeld een module 'Aboriginal Languages of New South Wales', eigendom van een door de gemeenschap bestuurde taalautoriteit die verantwoordelijk is voor het gevalideerde lexicon, de uitspraak, de etymologie, de culturele context en het lopende revitaliseringswerk. De eigenaren van de module behouden de autoriteit over de taal en het gebruik ervan, inclusief hoe de taal entiteiten in de natuurlijke wereld benoemt.

Een punt van domeinoverschrijdende autoriteit doet zich voor bij de *naamgeving van planten*. Elke plant in de botanische module kan — naast zijn wetenschappelijke naam — een inheemse naam uit het lexicon van de taalmodule dragen. Historisch gezien vielen deze inheemse namen onder de controle van de botanische module als bibliografische bijlagen. Een politiek besluit om de taalkundige soevereiniteit te herstellen, draagt de naamgevingsbevoegdheid over van de botanische module naar de taalmodule: vanaf nu is de canonieke inheemse naam voor een plant wat de taalmodule zegt dat het is.

10.2 Federatie als architectonisch antwoord

Het architecturale antwoord is een bilaterale federatie tussen de twee modules, met een manifest dat de afgebakende interactie precies benoemt:

- **Beperkt doel:** domeinoverschrijdende naamgevingsreferentie. De botanische module kan de taalmodule raadplegen voor de canonieke inheemse naam van een plant, gegeven een wetenschappelijke binomiale naam. De taalmodule behoudt alle zeggenschap over de naam; de botanische module behoudt alle zeggenschap over de wetenschappelijke taxonomie.
- **Gegevensstroom:** een gestructureerde query van de botanische module naar de taalmodule benoemt de wetenschappelijke binomiale naam; het antwoord is de canonieke inheemse naam (of `onbekend` als het corpus van de taalmodule die plant nog niet benoemt). De stroom is *pull-on-demand*; er is geen batchoverdracht geïmpliceerd. De botanische module kan antwoorden cachen met een door de tenant configureerbare vervaldatum.
- **Beleidsafhandeling:** de samenstelling van de taalmodule bepaalt het antwoord. Als het corpus van de taalmodule in herziening is en een naam voorlopig in afwachting is, draagt het antwoord die status als een `caveats_added-veld` op de proof-chain-vermelding; de botanische module maakt de status zichtbaar voor zijn gebruikers.
- **Intrekking:** beide partijen kunnen op elk moment intrekken. Intrekking wordt onmiddellijk doorgevoerd; de botanische module stopt met het stellen van vragen; opgeslagen reacties vervallen na hun vervaldatum. Er is geen gegevensstroom meer na intrekking.
- **Audit:** elke query en elk antwoord laat een ondertekende proof-chain-vermelding achter aan beide kanten. Elke partij kan de volledige federatiegeschiedenis reconstrueren vanuit haar eigen database.

10.3 De ervaring van de student

Een student die het lesprogramma doorloopt, stelt een vraag: *„Wat is de inheemse naam voor Eucalyptus camaldulensis?”* Het lesprogramma van het platform stuurt de vraag door naar de botanische module (die de wetenschappelijke binomiale naam als gezaghebbende bron bevat) en de federatie stuurt de subvraag over de naamgeving door naar de taalmodule. Het antwoord wordt *samengesteld uit een combinatie van gesitueerde taalmodules, niet uit een geavanceerd groot taalmodel.* De student ziet de naam, de bronvermelding van de taalmodule en een indicatie dat het antwoord door de federatie is verstrekt — niet omdat de federatie technisch interessant is voor een student, maar omdat verifieerbaarheid een kernwaarde van het curriculum is.

De architecturale eigenschap die hier op het spel staat, is dat de student een samengesteld gezaghebbend antwoord krijgt zonder dat er een LLM in de loop zit. Hallucinatie wordt structureel uitgesloten omdat geen enkel model het antwoord genereert op basis van een waarschijnlijkheidsverdeling over trainingsdata; het antwoord is een federatieve query tegen een samengesteld corpus dat wordt beheerd door de rechthebbende. Als het corpus geen antwoord heeft, geeft de federatie `'onbekend'` terug — de student krijgt te horen dat het systeem het niet weet, een structureel nauwkeurig antwoord dat de zelfverzekerde verzonnen antwoorden van een geavanceerd model niet kunnen bieden.

10.4 De architecturale lessen

Drie lessen vloeien uit dit uitgewerkte voorbeeld terug naar de architecturale verplichtingen van §5:

1. **Domeinoverschrijdende soevereiniteitsoverdracht is een federatie-operatie.** Wanneer de bevoegdheid over een klasse van referenties verschuift van de ene gemeenschap naar de andere (botanische → taalmodule voor plantennamen; iwi → kāhui voor een gedeeld kaupapa; parochie → bisdom voor een gedeelde evenementenkalender), bestaat de architecturale operatie uit het ondertekenen van een nieuw federatie- manifest, niet uit het migreren van gegevens tussen tenants. De gegevens blijven waar de rechthebbende zich bevindt; de federatie vertelt de consument waar hij zijn zoekopdracht moet uitvoeren.
2. **Het aanbieden van lesprogramma's via gefedereerde, gesitueerde modules is een structureel andere implementatie dan door LLM samengestelde antwoorden.** De use case voor het aanbieden van lesprogramma's is een sterke empirische drijfveer voor de voorkeur van de architectuur voor het aanbieden van inhoud zonder tussenkomst van LLM: waar de student een leerling is, moet het antwoord gezaghebbend zijn, niet probabilistisch.
3. **Het veld voor beperkt doel in het federatiemanifest is dragend.** Een federatie voor naamresolutie geeft de botanische module geen toestemming om het volledige corpus van de taalmodule te doorzoeken; het geeft alleen toestemming voor de genoemde queryvorm. De federatieservice van het platform weigert query's buiten de in het manifest aangegeven vorm. Dit is de architecturale eigenschap die twee soevereine gemeenschappen in staat stelt te federeren over een specifieke, afgebakende interactie zonder de autoriteit over

iets anders op te geven.

Een reeks verwante federatieklassen — tussen de collectiemodule van een museum en de module voor cultureel erfgoed van een inheemse gemeenschap; tussen de planningsmodule van een regionale raad en de module voor erfgoedsites hapū; tussen de curriculummodule van een schooldistrict en de taalmodule van een gemeenschap — hebben dezelfde vorm. Het voorbeeld Flora ↔ Talen wordt aangeboden als de canonieke illustratie omdat het zowel de dimensies *van datasoevereiniteit* als *de overdracht van epistemische autoriteit* tegelijkertijd zichtbaar maakt.

---

11. Zes dorpsachtige configuraties — voorbeelden uit een sjabloonfamilie

De architectuur wordt uitgedrukt via een sjabloonmodel. Een tenant- configuratie is geen eenmalige opbouw; het is een instantiatie van een sjabloon, waarbij de sjabloon de soevereine-record-primitieven, het beleidsoverervingsgedrag, de federatiesemantiek en de , de vorm van de governance-wachtrij, en de tenant-specifieke configuratie bepaalt wat de sjabloon openlaat: de grondwet, de lidmaatschapsstructuur, de subgroepstopologie, de meertalige locale, het cohort van de gesitueerde-taal-laag, de leveranciersvoorkeuren binnen de leveranciersverbod-envelop.

De operationele waarde van het sjabloonmodel is dat een nieuwe dorp-type configuratie een configuratieoefening is, geen herbouw. De architecturale waarde is dat een beoordelaar die één dorp-type configuratie onderzoekt, *dezelfde architectuur* onderzoekt waarop elke andere dorp-type configuratie ook draait; de soevereiniteitseigenschappen zijn uniform binnen de familie omdat het sjabloon uniform is.

Het platform dat in dit artikel wordt beschreven, is zelf de referentie-implementatie van de architectuur die het beschrijft. Het platform is gebouwd door een klein team in Nieuw-Zeeland, onder leveranciersverbod en soevereiniteitsbeperkingen — dezelfde beperkingen waartegen de architectuur zich verdedigt. Het bouwen onder die beperkingen bracht de faalmodi aan het licht waartegen de architectuur bescherming biedt, waaronder de verleiding om, onder kostendruk, terug te vallen op infrastructuur onder Amerikaanse jurisdictie voor opslag of rekenkracht. De weerstand van de architectuur tegen die verleiding, waargenomen tijdens de bouw, is op zichzelf al een bijdrage die dit artikel documenteert.

De sjabloonfamilie is operationeel: configuraties van het type 'village' draaien op infrastructuur onder EU-soevereiniteit (OVH Frankrijk) en infrastructuur onder Nieuw-Zeelandse soevereiniteit (Catalyst Cloud). Specifieke subdomeinnamen van tenants worden in dit artikel niet opgesomd en zijn opzettelijk weggelaten om de blootstelling van het aanvalsoppervlak te verminderen; ze zijn beschikbaar voor legitieme recensenten via een rechtstreeks verzoek aan de corresponderende auteur. Elke momenteel operationele configuratie van het dorpstype verifieert zijn leden en retourneert een 302/403-antwoord op niet-geverifieerde verzoeken om inhoud — het operationele kenmerk van een live tenant. Er wordt een carpool-configuratie gebouwd op infrastructuur onder Nieuw-Zeelandse soevereiniteit als de eerste beoogde multi-

instance federatie-implementatie; carpool isoleert federatie- en administratieve backend-primitieven zonder het volledige, naar leden gerichte oppervlak van andere dorpstypen, wat het de duidelijkste pedagogische weergave van de federatie-primitief maakt. De uitnodiging aan gemeenschappen of organisaties die geïnteresseerd zijn in deelname aan de pilot staat in §7.4.

Village model	Doel (een selectie uit mogelijke toepassingen)
Whānau	Māori -sites voor uitgebreide families met intergenerationeel genealogisch en m
Rūnanga	Iwi (stam)raadsites met notulen, commissiebesluiten en taonga die rechtstreeks
Commissie	Overlegorganen voor sportfederaties, beroepsverenigingen en lokale genootsch
Kāhui Māori	Coördinatiesitesiwi waar het delen plaatsvindt via bilaterale federaties tussen s
Bestuur	Institutionele organen (gemeenschapsbesturen, schoolbesturen, parochieraden)
Lidmaatschap	Nationaal aangesloten organen met lokale afdelingen — een nationale verenigin

De hier ontwikkelde typologie generaliseert verder dan dorpstypen naar een bredere klasse van organisatievormen waarvan de structurele belangen niet individueel maar collectief worden verwoord. Sectorale medezeggenschapsorganen in rechtsgebieden waar collectieve onderhandelingen grondwettelijk zijn verankerd — ondernemingsraden onder de Mitbestimmungsgesetz in Duitsland, vertegenwoordigende raden onder de Oostenrijkse Arbeitsverfassungsgesetz, de Belgische ondernemingsraad, Scandinavische samarbejdsudvalg-regelingen — zijn georganiseerde vormen waarvan de belangen op het gebied van gegevenssoevereiniteit niet worden gediend door individuele rechten van betrokkenen alleen. Coöperatieve verenigingen, waar lidmaatschapsrechten gelijkwaardig zijn en beslissingen worden genomen door ledenvergaderingen, hebben dezelfde architecturale vereisten: bilaterale federatie tussen coöperaties in verschillende rechtsgebieden; soevereine gegevensbestanden met door leden gestuurde overdraagbaarheid; een gebruikersinterface voor stakeholderbestuur die collectief overleg ondersteunt. Vakbonden in rechtsgebieden waar vakbondsvertegenwoordiging institutioneel verankerd is, hebben dezelfde vorm. De architectuur legt geen enkele specifieke bestuursvorm op; ze legt de basiselementen bloot die een dergelijke vorm vereist.

Aanvullende dorpstypen in de sjabloonfamilie — familie (gericht op genealogie), parochie (lokale kerkgemeenschap), bedrijf (ledenlijst plus mededelingen voor kleine verenigingen van handelaren) en carpool (ritbemiddeling, in ontwikkeling, drager van de beoogde eerste multi-instance federatie-implementatie) — zijn concrete voorbeelden van dezelfde sjabloonfamilie. De set is geen vaste lijst; de waarde van de sjabloon is juist dat aanvullende dorpstypen kunnen worden geconfigureerd zonder architecturale wijzigingen.

11.1 Situatiespecifieke taalcohorten (verwijzing naar Paper B)

Elke configuratie van een dorpstype wordt gekoppeld aan een cohort *van de gesitueerde taallaag* — een taalmodel per huurderstype dat is getraind op de eigen inhoud van de huurder met strikte trainingsdiscipline. Cohorten worden ingezet voor de dorpstypen die momenteel in productie zijn; aangewezen cohorten voor aanvullende dorpstypen wachten op de eerste huurder van elk type voordat ze in

gebruik worden genomen, volgens de projectdiscipline tegen ambitieuze training. De empirische bevindingen — waaronder een gedocumenteerde reeks experimenten met gewichtsaanpassingen die uniforme verslechtering aantonen, de vier “no-X”-regels voor de hygiëne van trainingsgegevens, de CPU-fallback-inferentiearchitectuur en de evaluatieresultaten per cohort — worden afzonderlijk gerapporteerd in de samenvatting van Paper B.

Er is een pre-launch gate op platformniveau: het aanmaken van tenants wordt geblokkeerd totdat de operator expliciet toestemming heeft gegeven. Het platform start geen tenants stil; de poort zorgt ervoor dat elke operationele tenant een autorisatiestap heeft doorlopen die zelf in een auditlog wordt vastgelegd. Een afzonderlijke poort voor soevereine constitutie dwingt een harde 403 af voor tenants die na 01-05-2026 zijn aangemaakt en die de vereiste soevereine secties missen; deze poort is operationeel met ingebouwde opschortingsimmuniteit voor aangewezen platform-infrastructuur-tenants.

---

12. Evaluatie

In dit hoofdstuk wordt het bewijsmateriaal van de implementatie van de architectuur in één hoofdstuk verzameld. Er worden drie ledgers en één casestudy gepresenteerd: het use-case-verificatieledger, het framework-consultatieledger, de snapshot van de implementatie en verificatie, en de casestudy over hash-stabiliteit in de hydratatiemodus van 22-04-2026.

12.1 Experimentele opstelling

Het platform draait in productie op twee infrastructuurlocaties: een EU-soevereine implementatie op OVH Frankrijk (community.myfamilyhistory.digital en bijbehorende subdomeinen van tenants onder mysovereignty.digital en myfamilyhistory.digital) en een Nieuw-Zeelandse soevereine implementatie op Catalyst Cloud (village-nz-infrastructuur die de subdomeinen van tenants van mysovereignty.digital bedient). Beide locaties draaien dezelfde code met dezelfde revisie; de spiegelpariteit wordt gehandhaafd tussen twee implementatiedoelen plus een zelfgehoste Forgejo-upstream. De database is per locatie MongoDB met tenant-gebonden query's afgedwongen door een Mongoose-plugin; runtime-inferentie voor de situated-language-laag wordt gehost op een Nieuw-Zeelandse soevereine GPU (Catalyst A6000 tijdens kantooruren, home-eGPU buiten kantooruren) met automatische failover.

12.2 Verificatie van use-cases ledger

Het use-case-ledger toont aan dat elke geïmplementeerde component werkt zoals ontworpen tegen een live lokale database. Het ledger omvat de architecturale componenten: herkomstcanonicalisatie; de Policy Inheritance Engine en de bijbehorende filtermodi; verificatiecaching; het ondertekenen van de proof-chain, inclusief UPDATE en DELETE in query-modus; het tombstone-pad van de governance-wachtrij; DID-publicatie; de export-wrapper inclusief de zichtbaarheidsoverlay;

constitutionele voorwaarden; het federatieoppervlak; migratie van soevereine records tussen de door tenants gegenereerde inhoudsmodellen en dekking van ingebedde subdocumenten; bedrading op groepsniveau, inclusief het chat-thread-oppervlak; DSR-canonieke export- en ingest-paden; afstemming van het werkersbeleid; WebSocket-beleidsaanpassing; tombstone-retrofit; proof-chain-compactie; het access-gate-oppervlak; de per-tenant-viewerpagina's. Het PASS-percentage van het grootboek is gelijk aan de pariteit op het moment van de snapshot; de scriptset is reproduceerbaar door een externe beoordelaar met toegang tot de codebase (bijlage B geeft een overzicht van de categorieën).

12.3 Framework-consultatie ledger

Het ledger voor raamwerkconsultatie bestrijkt het architecturale oppervlak. Elk record vermeldt de geraadpleegde dienst, het oordeel per voorwaarde en de operationele metadata (naam van de bewerking, duur, resultaatklasse). De set actieve diensten omvat de kernservices Tractatus (BoundaryEnforcer, ContextPressureMonitor, MetacognitiveVerifier, PluralisticDeliberationOrchestrator, CrossReferenceValidator, InstructionPersistenceClassifier) plus een bredere reeks beslissingsspecifieke diensten die zijn opgebouwd naarmate de architectuur is gegroeid (Tractatus, SovereigntyPrimacyEnforcer, PolicyCoherenceValidator, TenantIsolationValidator, AuditTrailVerifier, SchemaGuardian, PolicyDecisionOracle, TenantOwnerAuthority, PluralisticDeliberator, GovernanceOrchestrator). Het grootboek wordt uniform vastgelegd in lokale en in door de EU en Nieuw-Zeeland beheerde productiedatabases — drie opslaglocaties per raadpleging — zodat het verlies van één enkele host de auditpositie niet in gevaar brengt. Een geplande gezondheidscontrole rapporteert de actualiteit van raadplegingen per dienst ten opzichte van drempels die zijn afgestemd op een realistisch werkritme (4 uur voor het hele systeem, 24 uur per dienst); deze drempels hebben de eerdere standaardinstellingen van 30 minuten vervangen, die vals-positieve waarschuwingen veroorzaakten bij elke korte onderbreking in de actieve ontwikkeling.

12.4 Implementatiestatistieken

Implementatiestatus op het moment van de snapshot: beide productiesites rapporteren `/api/health` 200; de services van de frameworkmodule rapporteren operationeel op beide sites; verify-and-cache draait 's nachts over de door tenants gegenereerde contentmodellen; de Catalyst-smoke-test (catalyst-operational) slaagt met volledige dekking; ESLint draait foutloos over de gewijzigde bestanden bij elke implementatie; de spiegelpariteit wordt gehandhaafd tussen `ovh`, `catalyst` en `forgejo`. Het smoke-test FAIL-oordeel dat wordt waargenomen tijdens actieve onderhoudsvensters is verwacht gedrag — de smoke-test vraagt productie-eindpunten op die onderhouds-HTML serveren tijdens de lock-out — en wordt hersteld naar PASS zodra het onderhoudsvenster wordt opgeheven.

12.5 Verifieerbaarheid van de cache De

De verificatiecache wordt gevuld voor de operationele tenantset op beide productiesites en omvat de elf inhoudstypen die momenteel actief in gebruik zijn. Records zonder

herkomst-hash (een klein restant van legacy-records van vóór de migratie naar sovereign-records) worden gemarkeerd als `niet-verifieerbaar` in plaats van `geldig`. De architecturale eigenschap is dat het verificatieveld in elke API GET- respons de cache-status aan consumenten toont; downstream-auditingtools kunnen de verificatie-status van de architectuur afleiden door de API-interface te bevragen, zonder dat database-toegang nodig is. De wezenlijke bijdrage is de discipline van observeerbaarheid, niet het aantal records.

12.6 Casestudy: de hash-stabiliteitsbug in de hydratatiemodus van 22-04-2026

Het meest leerzame empirische voorval tijdens de ontwikkeling van de architectuur was de ontdekking van een bug in de hash-stabiliteit tijdens de validatie van gebruiksscenario's voor de integratie van het leespad in de verificatiecache. De serializer voor de canonieke vorm doorliep de opsombare eigenschappen van een ORM-subdocument — een patroon dat correct werkte voor payloads met gewone objecten, maar de interne ORM-status blootlegde voor gehydrateerde documenten, waardoor hashes werden geproduceerd die verschilden tussen de hydratatiemodi. Hashes bij het opslaan slaan één waarde op; hashes bij het lezen berekenen een andere; elk record na de implementatie zou `een 'chain_hash_mismatch'` vertonen. De oplossing was een normalisatiestap van één regel. De bug was de unit-testsuite zonder problemen gepasseerd omdat de tests gewone objecten simuleerden — de foutmodus vereiste echte gehydrateerde documenten.

Dit is een sprekend voorbeeld van de werkwijze: tests bewijzen dat de bedrading werkt in mocks, maar use-case-validatie tegen een live database bewijst dat de bedrading in de praktijk werkt. De werkwijze dat tests bewijzen wat mocks onthullen, en dat use-case-validatie aan het licht brengt wat mocks verbergen, is vastgelegd in de werkwijze van het project en is de reden waarom er naast de unit-testsuite een set use-case-validatiescripts bestaat. Na de fix werden alle bestaande productierecords opnieuw in de cache opgeslagen met de gecorrigeerde serializer in canonieke vorm; er ging geen enkel record verloren, geen enkele auditpositie kwam in het gedrang en de bug is het canonieke voorbeeld dat wordt gebruikt in trainingen over de werkwijze.

12.7 Interpretatie

Het evaluatiebewijs ondersteunt een specifieke bewering: de architectuur is operationeel, waarneembaar en controleerbaar op het API-oppervlak over meerdere soevereine infrastructuurlocaties heen. Het verificatieoppervlak (use-case-ledger, framework-consultation-ledger, implementatiestatistieken) is reproduceerbaar door elke beoordelaar met toegang tot de codebase; de casestudy over hash-stabiliteit toont aan dat de operationele discipline echte faalmodi opvangt die door mock-tests worden gemist. Wat de evaluatie *niet* beweert, is dat elke dreiging in §4 volledig wordt afgeweerd — de architectuur verdedigt *benoemde* invarianten met *benoemde* predikaten; dreigingen buiten het model (aanvallen met ontkenbare versleuteling; compromittering van de toeleveringsketen van het framework Tractatus; fysieke compromittering van de hardware van de inferentielayer) vallen buiten het bereik en worden in de operationele discipline bijgehouden als afzonderlijke aandachtspunten.

13. Open-sourcehouding

De open-sourcehouding onderscheidt twee aspecten.

Het **Tractatus** — het governancemechanisme voor de ontwikkelingstijd — is openbaar, open source onder de Apache 2.0-licentie en wordt verspreid via `codeberg.org/mysovereignty/tractatus-framework` [1]. Het werkdocument, de codepatronen en de metrics zijn reproduceerbaar door een externe beoordelaar met toegang tot een installatie van de klasse Claude-Code en de patroonbibliotheek van het framework.

De codebase van het platform — de runtime-applicatie — wordt module voor module als open source uitgebracht onder de European Union Public Licence Version 1.2 (EUPL-1.2) [10]. Bronbestanden bevatten per bestand EUPL-1.2-headers; de meest recent gewijzigde bestanden van het platform (herkomst, verificatiecache, attributie op groepsniveau, query-mode verwijder- en update-hooks, DSR-canonieke export, federatiediensten, UI-componenten voor belanghebbenden, beleidshelpers voor workers) dragen de header. De licentie op repository-niveau is in afwachting van de oprichting van een bestuursorgaan volgens Nieuw-Zeelandse wetgeving, met een democratisch gekozen raad van bestuur en een adviescommissie. De raad keurt architecturale wijzigingen goed die van invloed zijn op het open-sourcebeleid van het platform en de toezeggingen aan belanghebbenden; de adviescommissie geeft advies over cultuur en belanghebbenden (Māori cultureel advies; advies van minderheidstaalgemeenschappen; FOSS-gemeenschap advies). De raad is nog niet samengesteld; de EUPL-1.2-headers per bestand zijn de lopende open-sourcevoorbereiding, niet de definitieve status op repository-niveau.

Er is bewust gekozen voor een releasepad per module in plaats van een volledige repository-release. De reden hiervoor is een categorie aanvalsoppervlakken van grote taalmodellen, waarbij een volledige bronrelease van een intern gekoppeld platform materiaal blootlegt waarvan het dreigingsmodel niet is beoordeeld op de modulegrens — code die alleen weerstand biedt tegen bepaalde aanvallen omdat deze nog niet is gelezen door modellen die zijn getraind op vijandige corpora. Een zorgvuldige release per module zorgt ervoor dat het dreigingsmodel van elke module vóór publicatie kan worden beoordeeld, en beperkt het doorsijpelen van interne koppeling naar oppervlakken die afhankelijk zijn van externe factoren. De tot nu toe vrijgegeven modules — de kernplugin voor soevereine records, de Policy Inheritance Engine, de tenant-sleutelopslag, het Tractatus, componenten van de DSR- pijplijn — vormen het architecturale oppervlak dat externe beoordelaars kunnen gebruiken; volgende modules volgen hetzelfde ritme van eerst beoordelen en dan vrijgeven.

Er bestaat een concept van Village Model Licence als een aangepaste licentieformule die bedoeld is om FOSS-typische toestemmingen te combineren met specifieke clausules ter bescherming van de gemeenschap (geen gebruik voor het surveilleren van gemeenschappen; geen gebruik dat in strijd is met de bepalingen inzake gegevenssoevereiniteit van een gemeenschap; geen gebruik dat de door een tenant verklaarde CARE-Principles-houding zou omzeilen). Het ontwerp wacht op formele

juridische beoordeling; in afwachting van de uitkomst van de beoordeling blijft de licentie per bestand van het platform EUPL-1.2.

13.1 Leveranciersdiscipline

Het platform maakt geen gebruik van Amerikaanse cloud-, SaaS- of infrastructuur afhankelijkheden in zijn productieverzoekpad. EU-soevereine hosting is OVH Frankrijk; Nieuw-Zeelandse soevereine hosting is Catalyst Cloud (met Catalyst (NZ) Limited als de bedrijfsentiteit); home-eGPU-failover voor inferentie buiten kantooruren vindt plaats op een niet-Amerikaanse grafische verwerkingseenheid. De hosting van de coderepository is gesplitst: een zelfgehoste Forgejo-instantie is de EU-soevereine primaire remote, met mirrors naar de OVH- en Catalyst-bare repositories. Voor de verwerking van betalingen wordt Airwallex (NZ) Limited gebruikt — Amerikaanse kaartnetwerken worden alleen per transactie geraakt wanneer de kaartuitgever van de betaler in de VS is gevestigd, en alleen voor die ene transactie. Voor vertaaltools wordt gebruikgemaakt van DeepL (Duitse entiteit, onder de jurisdictie van de EU-AVG). Deze leveranciersdiscipline wordt afgedwongen door een interne regel die toegestane en verboden aanbieders expliciet opsomt; afwijkingen vereisen een expliciete beslissing op projectniveau , geen stille introductie.

Er worden geen biometrische gegevens verzameld door het platform. Identiteitsverificatie van leden bij operaties met hoge inzet wordt uitgevoerd buiten het platform om (persoonlijke kennismaking binnen de gemeenschap; video kennismaking; verificatie via papieren kanalen) of via de door het lid beheerde decentrale identificatiesleutel, nooit via biometrische registratie. De redenering is structureel en komt samen vanuit vier invalshoeken: biometrische gegevens zijn onherroepelijk, dus een lek kan niet worden verholpen door rotatie; biometrische gegevens hebben drie structurele blootstellingsroutes binnen de Amerikaanse jurisdictie (directe registratie aan Amerikaanse zijde bij grenzen en visuminterviews; hosting in Amerikaanse cloud onderworpen aan dwang van de CLOUD Act, ongeacht de nationaliteit van de betrokkene; toekomstige Enhanced Border Security Partnership-regelingen die voorzien in directe databasetoegang tot biometrische opslagplaatsen van partnerlanden); Māori biometrische en DNA-gegevens vallen onder specifieke Te Tiriti / WAI 262 / WAI 2522 bescherming die van kracht wordt zodra dergelijke gegevens door het platform worden verzameld, en de blootstelling van die gegevens door de Kroon aan een buitenlands jurisdictioneel regime stelt de bescherming van taonga onder artikel 2 op de proef op manieren die het platform niet mag uitsluiten; en de meest ergonomische biometrische applicatieprogrammeerinterfaces worden beheerd door bedrijven met hoofdkantoor in de VS waarvan het gebruik in elk geval in strijd zou zijn met de leveranciersverbodsregel van het platform. Door te weigeren biometrische gegevens te verzamelen, wordt het platform architectonisch uit dit hele risicovlak verwijderd — de exploitant kan niet worden gedwongen om openbaar te maken wat nooit is verzameld. Leden die gebruik willen maken van apparaatgebonden biometrische ontgrendeling van hun eigen inloggegevenskluis, kunnen dat doen op hun eigen hardware; de biometrische gegevens overschrijden nooit de grenzen van het platform, en het platform mengt zich niet in dit patroon. Het eigen toegangsoppervlak van het

platform — inclusief de meegeleverde soevereine toegangspoort (§15), per tenant ingeschakeld op het tempo van de operator — maakt gebruik van tekstwachtzinnen (dice-words / EFF-woordlijststijl; hoge entropie en vervangbaar) plus zelfgehoste proof-of-work botdetectie.

13.2 De IP-perimeter

De publicatiehouding maakt een onderscheid tussen de *architecturale vorm* (publiceerbaar als paperinhoud; gepubliceerd als open-source modules) en de *operationele details* (achtergehouden om redenen van de IP- perimeter). Achtergehouden: specifieke Tractatus per dienst (de catalogus is de bijdrage van het framework); per-producttype vocabulaire-inhoud buiten de hoogwaardige sjabloon familie; per-tenant configuratiespecificaties; specifieke federatie manifest veldsetdetails buiten de architecturale vorm in Bijlage C. Gepubliceerd: de architecturale primitieven in het artikel; het dreigingsmodel en testbare predikaten; de hoogwaardige schema-vormen; de beperkingen en storingsmodi (§15); de bronmodules volgens het module-voor-module releaseplan.

---

14. De architecturale bijdrage

De architectuur is een reactie op een structurele situatie, geen concurrerend product. Het standaard community-platformmodel — in Amerikaanse handen, aandacht trekkend, met naar believen herzienbare servicevoorwaarden — is een specifieke architecturale keuze over waar gegevenssoevereiniteit ligt. Een architecturale keuze kan alleen worden beantwoord door een architecturaal alternatief, niet door herzieningen van de servicevoorwaarden of toevoegingen van functies aan bestaande platforms.

Vier eigenschappen van het werk zijn hierbij van belang.

Het werk is **operationeel**. De architectuur is geen specificatie die wacht op implementatie. Het draait, in meerdere dorpachtige configuraties, op infrastructuur die onder de soevereiniteit van de EU en Nieuw-Zeeland valt. Een beoordelaar kan de operationele status verifiëren via de API-interface en elke architecturale beslissing verifiëren via het permanente framework-consultatieledger. Het use-case-verificatieledger dekt de geïmplementeerde architecturale interface op pariteit. De wezenlijke bijdrage is de discipline van het vastleggen — dat de architectuur auditartefacten produceert die van buitenaf waarneembaar zijn zonder op het woord van de operator te hoeven vertrouwen.

Het werk is **structureel overdraagbaar**. De architectuur gaat niet specifiek uit van Māori, te reo Māori of Te Tiriti. Hetzelfde `metadata.origin.collective_id-veld` waarmee een Māori een record aan haar rūnanga kan toewijzen, stelt een een Welshe gemeenschap een record aan haar parochie toe te wijzen, een Sámi-gemeenschap aan haar siida, een Sorbische gemeenschap aan haar dorp. Het situated-language-layer-patroon is op dezelfde manier overdraagbaar: een Welshe-taal laag die is getraind op Welshe-taalmateriaal onder het gezag van de Welshe gemeenschap

beantwoordt Welshe vragen met dezelfde architecturale houding als de Māori laag Māori beantwoordt. De architectuur is een substraat, geen product.

Het werk is **geschikt voor federatie**. De infrastructuur voor bilaterale federatie wordt end-to-end geleverd met een uitgebreide negatieve-testmatrix die het toepassingsgebied, schrijfblokkering, audit, citatiediscipline, caching, randgevallen, autorisatie en fase-3-naamruimtescheiding omvat. Live federatiekoppelingen tussen onafhankelijke tenant-implementaties zijn in afwachting van de eerste multi-instance-implementatie; de architecturale eigenschap — dat twee gemeenschappen, op door hen gespecificeerde voorwaarden, kunnen instemmen met een specifieke, afgebakende interactie, en alleen dat — is precies wat de drie artikelen van Te Tiriti impliceren voor digitale infrastructuur, en wat minderheidstaalgemeenschappen in Europa nodig hebben wanneer hun gemeenschapsoverschrijdende werk juridische jurisdicties overbrugt.

Het werk **respecteert de overdraagbaarheid**. Een lid is een eersteklas betrokkene. Zij kunnen hun volledige gegevensset exporteren in cryptografisch verifieerbare vorm en deze migreren naar elke andere tenant die onder hetzelfde architecturale model opereert. De export is symmetrisch met het recht op inzage uit artikel 15 van de AVG; de migratie is symmetrisch met de architecturale toezegging dat uittreding een eersteklas operatie is. Een gemeenschapsmodel waarin uittreding moeilijk is, is een gesloten tuin, ongeacht de marketingtaal die wordt gebruikt; een gemeenschapsmodel waarin uittreding architectonisch is, is wat het hier gerapporteerde werk beschikbaar maakt.

De inhoudelijke stelling van de architectuur is dat een platform op gemeenschapsschaal zo kan worden gebouwd dat de soevereiniteitseigenschappen op het niveau van de records en de tenant-infrastructuur liggen, en niet aan het oordeel van de operator. Het standaardmodel is afhankelijk van door de operator verleende en door de operator intrekbare soevereiniteit; een architectonisch alternatief — soevereiniteit als eigenschap van de records en de tenant-infrastructuur — wijst die voorwaarde bij opzet af. Het hier beschreven werk is een concreet bewijs dat een dergelijk alternatief kan worden gebouwd door een klein team in Nieuw-Zeeland, met een klein budget, en in productie kan worden genomen voor echte gemeenschappen, zelfs nu de regelgeving steeds meer neigt naar doorgrijping door buitenlandse jurisdicties (het Enhanced Border Security Partnership is hiervan het actuele voorbeeld in Nieuw-Zeeland).

---

15. Beperkingen en storingsmodi

Verschillende punten vallen binnen de reikwijdte van de beweringen in dit document, maar zijn op het moment van dit concept nog niet geïmplementeerd:

- **Live carpool-federatieverkeer.** De bilaterale federatie-infrastructuur wordt end-to-end geleverd met een aanzienlijk verificatieoppervlak, maar er is nog geen live federatie tussen onafhankelijke tenant- implementaties geactiveerd. De carpool-federatie-implementatie, beschouwd als de eerste multi-instance-illustratie, verloopt op het tempo van de operator.

- **Tier-2-cohorten op de gesitueerde-taal-laag.** Aangewezen cohorten voor aanvullende dorpstypen worden opgeschort volgens de projectdiscipline tegen ambitieuze training: een cohort wordt pas in gebruik genomen als de eerste tenant van dat type in implementatie is.
- **Volledige open-source release op repository-niveau.** De EUPL-1.2-headers per bestand van het platform zijn aanwezig; de release per module loopt; de licentie op repository-niveau is in afwachting van goedkeuring door de Raad , en de Raad zelf is in afwachting van oprichting als rechtspersoon volgens de Nieuw-Zeelandse wetgeving.
- **Publicatie van de Tiriti Compliance Statement v0.2.** Er bestaat een v0.2-herziening op basis van het door de operator gedelegeerde, op eigen inzicht gebaseerde oordeel; voor de genoemde publicatie is de uitdrukkelijke toestemming van Dr. Taiuru vereist.
- **Formele juridische beoordeling van deVillage Model Licence.** Het ontwerp bestaat; de formele juridische beoordeling is in behandeling; in afwachting van de uitkomst blijft de licentie per bestand van het platform EUPL-1.2.
- **Identiteitsafstemming van ontvangende tenant automatische onboarding.** Het huidige DSR-migratie-ingestpad weigert standaard automatische onboarding; automatische onboarding via tenantoverschrijdende DID is een beveiligingsrisico dat een eigen ontwerpronde vereist.
- **Soevereine toegangspoort (wachtwoordzin + soevereine proof-of-work botdetectie + papieren herstelcodes) — geleverd, uitrol per tenant op het tempo van de operator.** De basisauthenticatie van het platform bestaat uit httpOnly-cookies plus isolatie van de tenantcontext, afgedwongen op het databasequery-niveau. De access-gate-component wordt end-to-end geleverd als globale request-pipeline-middleware (`accessGate`) met een per tenant `AccessGateConfig` (wachtwoordzin-hash, rotatiegeschiedenis, aantal herstelcodes), tien REST-eindpunten (`/api/access-gate/{status, pow/{challenge,verify}, passphrase/verify, recovery/use, admin/{enable,disable,rotat codes/pdf}}`), een zelfgehost proof-of-work challenge/verify-paar (geen externe botdetectieservice) en op papier afdrukbare herstelcodes die op verzoek van de operator worden gegenereerd als PDF op verzoek van de operator (geen sms, geen e-mail, geen out-of-band kanaal gerouteerd via Amerikaanse infrastructuur). De component is standaard uitgeschakeld voor elke tenant; de uitrol per tenant — het uitgeven van wachtzinnen, de distributie van herstelcodes en de onboarding van leden bij de gate — verloopt in het tempo van de operator en vindt tenant voor tenant plaats onder gedocumenteerde toezicht. De architecturale toewijding aan uitsluitend tekstgebaseerde en niet-biometrische authenticatie, zoals vastgelegd in §13.1's leveranciersdiscipline en §4's invariabele I9, is permanent en wordt vandaag de dag afgedwongen door het bestaande 'geen biometrische gegevens verzamelen'-beleid van het platform, onafhankelijk van de uitrolstatus van de gate per tenant. Architecturale afwijzingen die expliciet zijn voor het ontwerp van de poort — biometrische authenticatie, op sms gebaseerde tweefactorauthenticatie, magische links via e-mail via in de VS gehoste providers, door de VS gecontroleerde push-OTP, door de VS gecontroleerde botdetectiediensten, gedragsbiometrie — zijn gedocumenteerd in het plan van aanpak voor de toegangspoort, samen met de redenering achter elke afwijzing, zodat het keuzeoppervlak permanent is in

plaats van een vergissing. Wat door de operator wordt bepaald, is de beslissing om de functie per huurder in te schakelen, niet het bestaan van de component.

- **Rechtspersoonlijkheid van AI-agenten — open vraag, behandeld in Paper B.** Dr Taiuru (2026) [25a] stelt, als een open vraag, of en onder welke voorwaarden rechtspersoonlijkheid zou kunnen worden uitgebreid tot AI-agenten die zijn samengesteld uit Māori, waarbij hij de beslissing uitdrukkelijk uitstelt tot collectief werk tussen AI-ontwikkelaars, overheidsinstanties en Māori. Het bijbehorende Paper B rapporteert de discipline van cohorttraining op de gesitueerde taallaag waarop elk toekomstig partnerschapswerk per cohort zou voortbouwen; dit paper loopt niet vooruit op of bevooroordeelt dat werk.

Bedreigingen die buiten het §4-model vallen, worden apart bijgehouden binnen de operationele discipline: ontkenbare-versleutelingsaanvallen op de sleutelopslag; inbreuken in de toeleveringsketen van het Tractatus of de bijbehorende afhankelijkheden; fysieke inbreuken op de hardware van de inferentielayer; veroudering van cryptografische primitieven buiten het bereik van de algoritme-agility-wrapper. Geen van deze wordt in dit artikel behandeld; het zijn allemaal reële zorgen op implementatieniveau die een eigen analyse verdienen.

Twee structurele beperkingen zijn inherent in plaats van implementatiegerelateerd. De architectuur behoudt de soevereiniteit van de gemeenschap over gegevens; zij behoudt op zichzelf niet de soevereiniteit van de gemeenschap over *cognitie*. Een gemeenschap die de situated-language-laag gebruikt om vragen van leden te bemiddelen, maakt nog steeds gebruik van een taalmodel; het trainingscorpus, de trainingsdiscipline en het runtime-gedrag van het model maken deel uit van de oppervlakte van de architectuur, en staan er niet los van. Paper B zal de empirische trainingsdiscipline documenteren die de situated-language-laag betrouwbaar maakt voor gebruik door de gemeenschap; de bevindingen daarvan beperken de conclusies die een lezer kan trekken uit dit paper alleen. De andere structurele beperking is dat de verdediging van de architectuur tegen §4's tegenstander A1 (juridisch gedwongen hostoperator) uiteindelijk afhankelijk is van het feit of de tenant zijn eigen infrastructuur exploiteert of samenwerkt met een host met soevereine jurisdictie: de architectuur kan geen soevereiniteit creëren waar de jurisdictie van de host dit niet ondersteunt, maar ze kan wel soevereiniteit behouden voor tenants waarvan de hosts zelf onder een soevereine jurisdictie vallen.

---

16. Conclusie

De hier beschreven architectuur is geïmplementeerd en draait op infrastructuur onder de soevereiniteit van de EU en Nieuw-Zeeland. De kern primitieven zijn operationeel: isolatie van huurders als de fundamentele primitief; uniforme metadata van soevereine records in de door huurders gegenereerde inhoudsmodellen; cryptografische herkomst met algoritmische flexibiliteit; beleidsopvolging met effectieve beleidsbeperking bij de leesgrens; proof-chain-ondertekening bij aanmaken, bijwerken en verwijderen (zowel in documentmodus als query-modus); verificatiecaching die zichtbaar wordt bij het lezen; sleutelopslag per tenant met definitieve cryptografische verwijdering; publicatie van gedecentraliseerde identificatie;

governance-wachtrij met ondertekend beslissingsspoor; export-wrapper met overlay voor zichtbaarheid voor niet-beheerders en symmetrische auditlogging; bilaterale federatie met ondertekend manifest; door leden aangestuurde soevereine overdraagbaarheid met Artikel-15-symmetrische opname door ontvangende tenant; per-tenant-type gesitueerde-taallaag; stakeholder-governance-UI met alleen-lezen beoordelingsoppervlak (Fasen 1–5) plus de geleverde fase-6-superviseerde participatieve dialooginterface (door de operator goedgekeurde redactionele wachtrij, opstellen-en-publiceren-poort, geen automatische publicatie), gegeneraliseerd over de producttypes van het platform in fase 7; afstemming van werknemers- en WebSocket-beleid; proof-chain-compactie primitief; tombstone-retrofit-primitief; en de geleverde soevereine toegangspoort (tekstwachtwoord + zelfgehoste proof-of-work-botdetectie + papieren herstelcodes; per tenant uitgerold op het tempo van de operator).

Het framework-consultatieledger bestrijkt het architecturale oppervlak (elk overleg wordt uniform vastgelegd in lokale plus EU- en NZ-soevereine productiedatabases); het use-case-verificatieledger bestrijkt de geïmplementeerde architecturale componenten op pariteit; bilaterale federatie- infrastructuur wordt end-to-end geleverd met een uitgebreide negatieve-test matrix (een subset die bovendien wordt doorlopen door een live multi-tenant validator), met live federatiekoppelingen tussen onafhankelijke tenants in afwachting van de eerste multi-instance carpool-activering; de cohorten van de per dorpstype gesitueerde taallaag zijn operationeel; aangewezen cohorten voor aanvullende dorpstypen wachten op de eerste tenant van elk type alvorens in gebruik te worden genomen, volgens de projectdiscipline tegen ambitieuze training.

Het begeleidende artikel (Paper B — Situated Language Layers for Minority-Language and Indigenous Communities, synopsis van het empirische begeleidende artikel, gepubliceerd) beschrijft het architecturale patroon voor de cohorten met gesitueerde taallagen: AI's per gemeenschapstype die zijn getraind op de eigen gegevens van die gemeenschap, de werkingsprincipes die het project volgt bij het trainen en uitvoeren ervan, de Tier-1-implementaties die vandaag draaien, en de CPU-fallback-inferentiearchitectuur die het runtime-pad volledig buiten de door de VS gecontroleerde infrastructuur houdt. Het volledige empirische artikel — met evaluatie per cohort, ablaties voor gewichtsaanpassing, een scan van vergelijkende literatuur en een inhoudelijke verdieping in het bredere werk vandr. Taiuruop het gebied van Maori-AI-governance — zowel het Kaupapa Maori AI Framework [25b] (de prescriptieve, op Te Tiriti gebaseerde principes voor AI-toestemming, gegevenssoevereiniteit en volledige ketenverantwoordelijkheid) als het recentere onderzoek [25a] (de open vraag naar rechtspersoonlijkheid voor AI-agenten die zijn samengesteld uit Māori-kennis, die dr. Taiuru uitdrukkelijk overlaat aan collectief werk tussen AI-ontwikkelaars, overheidsinstanties en Māori -gemeenschappen) — wordt achtergehouden totdat geverifieerde trainingsgegevens beschikbaar zijn. Het volledige artikel is de plek waar de twee registers die Dr. Taiuru onderscheidt — de prescriptieve bestuursplicht en de interrogatieve vraag naar rechtspersoonlijkheid — rechtstreeks van invloed zullen zijn op de cohortdiscipline waarover wordt gerapporteerd. Het volledige artikel zal Meads Tikanga-test (tapu, mauri, take-utu-ea, whanaungatanga) gebruiken als het evaluatiekader waarop toekomstig samenwerkingswerk per cohort zich zou baseren; het loopt ook niet vooruit op

dat samenwerkingswerk, maar zal de cohorttrainingsdiscipline rapporteren in de empirische details die dergelijk samenwerkingswerk zou vereisen.

Het artikel wordt aangeboden als een uitgewerkt voorbeeld van hoe architecturale soevereiniteit een antwoord kan bieden op Te Tiriti, AI-persoonlijkheid (Dr. Taiuru 2026) en EBSP-jurisdictionele druk op het budget van een klein team. De architectuur is de bijdrage; de implementatie, de toewijding van de corresponderende auteur om de architectuur te laten draaien onder de beperkingen waartegen deze zich verdedigt, is het bewijs daarvan. Opmerkingen en correcties aan de corresponderende auteur zijn welkom.

Dankwoord

De auteur is Leslie Stroh dankbaar voor zijn fundamentele filosofische begeleiding op het gebied van pluralistisch denken en de vraag naar het goede in kunstmatige intelligentie. De toewijding aan pluralistische beraadslaging die als een rode draad door de bestuursarchitectuur van het platform loopt — en de bredere overtuiging dat een AI-substraat dat de moeite waard is om te bouwen, moet beantwoorden aan een inhoudelijk begrip van het goede, niet aan een procedureel begrip — dankt zijn vorm aan die gesprekken.

De auteur bedankt ook dr. Karaitiana Taiuruvoor zijnculturele veiligheidsbeoordeling van de Tiriti Compliance Statement v0.1; de vermelding van latere herzieningen wacht op zijn directe toestemming en wordt hier niet vermeld. Recensenten van vroege versies van het voorgaande implementatierapport (v0.4) hebben een kader geboden dat in dit artikel is overgenomen; hun bijdragen worden met dank erkend.

Bijlage A — Reproduceerbaarheid

Een recensent die de reproduceerbaarheid van de architectuur wil inspecteren, kan dit op de volgende niveaus doen.

Het Tractatus is de volledig openbare component, gedistribueerd op `codeberg.org/mysovereignty` `framework` onder Apache 2.0. Het werkdocument documenteert de observatiebevindingen van het framework en de architecturale patronen die het codificeert. Een recensent met toegang tot een Claude-Code-klasse-installatie kan de patroonbibliotheek van het framework reproduceren en de registratie van raadplegingen repliceren in een lokale database.

De vrijgegeven modules van het platform — onder EUPL-1.2 in de module-voor-module-release — vormen het architecturale oppervlak dat externe beoordelaars kunnen gebruiken. De modules omvatten tot nu toe de kern sovereign-record-plugin, de Policy Inheritance Engine, de tenant-sleutelopslag, componenten van de DSR-pijplijn en de infrastructuur voor het vastleggen van raadplegingen binnen het framework.

Architecturale componenten worden in dit document beschreven op het niveau van hun interacties en contracten. Specifieke bronpaden (bestandsnamen binnen de broncodeboom van het platform) worden opzettelijk niet opgesomd; reproduceerbaarheid op bestands- en regelniveau wordt gewaarborgd via de vrijgegeven modules, terwijl operationele details (implementatiepijplijn, onderhoudspoorten, hook-optimalisatie) worden achtergehouden als technische details in plaats van als onderzoeksbijdrage.

Verificatiescripts voor use-cases volgen een `validate-use-cases-*` naamgevingsconventie; opnamescripts voor framework-consultation volgen een `record-*-consultation` naamgevingsconventie. Elk consultatiescript produceert een idempotente invoeging van records in lokale plus EU-soevereine en NZ-soevereine productiedatabases op basis van een per-revisie identificatie.

De reproductie van het frameworkconsultatiepatroon, vanuit het Tractatus -framework, is gedocumenteerd in [1].

Bijlage B — Momentopname van het use-case-verificatieledger

Een actuele momentopname van het use-case-ledger omvat meer dan 45 verschillende validatiescripts. Elk script toetst een benoemde eigenschap van een architecturale component aan een live lokale database; de scripts zijn afzonderlijk en in hun geheel uitvoerbaar. De onderstaande categorieën geven een overzicht van de scriptset; het aantal scenario's per script en de PASS/FAIL-resultaten zijn opgenomen in de interne artefacten van het project en kunnen worden gereproduceerd door een externe beoordelaar met toegang tot de codebase:

- Canonicalisatie van herkomst en stabiliteit in verschillende hydratatiemodi
- Policy Inheritance Engine: kernresolutie; gate-and-filter-bedrading; origin-only-filtering; filtering op groepsniveau; strikte modus voor onbekend bereik Verificatiecaching: opnamedienst; post-save-hook + geplande
- Verificatiecaching: opnameservice; post-save hook + geplande sweep; read-path-integratie; update-path post-save hook
- Tenant-sleutelopslag: levenscyclusbewerkingen
- Ondertekening van bewijsketen: CREATE-consument; UPDATE/DELETE-documentmodus; DELETE-query-modus; UPDATE-query-modus; governance-wachtrij-tombstone
- DID-publicatie: tenant- + lid-documenten
- Aansluiting van governance-wachtrij
- Export-wrapper: gedrag per modus; integratie; auditlogboek voor succespad; zichtbaarheidsoverlay voor hash- en aggregate-modi
- Constitutionele vereisten en meertalige ondersteuning
- Migratie van soevereine records: over de door de tenant gegenereerde topniveaumodellen; dekking van ingebedde subdocumenten (NewsPost, Resource, EventMenu, Edition); subdocumentfasen 1+2
- Bedrading op groepsniveau en toewijzing tussen formulieren
- DSR-canonieke export: bundelassemblage; manifestondertekening; eerlijkheid van afkappingsvlag; end-to-end-opname bij ontvangende tenant
- Worker-beleidsgate: helper-unit-tests; integratie per worker (EmailProcessor,

DocumentScanner)
- WebSocket-beleidsadapter
- Tombstone-retrofit
- Compactie van de bewijsketen
- Federatie-oppervlak: negatieve-testmatrix over twaalf categorieën, met een subset doorlopen door een live multi-tenant validator

Bijlage C — Referentie van het federatiemanifestschema

Een federatieovereenkomstrecord bevat het bilaterale manifest op architectuurcomponentniveau. De schemanamen: de overeenkomst- identificatie; elke partij (tenant-identificatie, tenant gedecentraliseerde-identificatie, handtekening, tijdstempel van ondertekening); het afgebakende doel (een opsomming: carpool-match; gedeelde evenement-aankondiging; gezamenlijk overleg; kaupapa co-beheer; domeinoverschrijdende naamreferentie; en andere); de vorm van de gegevensstroom per richting (blootgestelde velden ; toegepaste transformatie; bewaring aan de ontvangende kant); de regel voor beleidsresolutie (welke grondwet is van toepassing; hoe beleidsconflicten worden opgelost, inclusief een expliciete tabel per veld); de intrekkingsprocedure (eenzijdig door een van beide partijen; onmiddellijke verspreiding; beide partijen bewaren ondertekende kopie in audit); en de audit-bewaaridentificatoren (cross-tenant query-logrecords aan beide kanten). Het manifest zelf bevat het standaard metadata-blok voor soevereine records (oorsprong, beleid, versleuteling, bewijsketen, verificatiecache); een federatie wordt niet geactiveerd zonder geverifieerde handtekeningen van beide partijen tegen hun respectieve DID- documenten.

Specifieke details over de implementatie van velden die buiten deze architecturale vorm vallen, worden achtergehouden volgens het IP-perimeterbeleid (§13.2). Beoordelaars die volledige schemaspecificaties nodig hebben voor compatibiliteitsevaluatie, kunnen deze verkrijgen via een rechtstreeks verzoek aan de corresponderende auteur onder de juiste vertrouwelijkheid.

Referenties

[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). *Distributive Equity Through Structure — A Community-Scale Worked Example of Values Stickiness, 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). The CARE Principles for

Indigenous Data Governance. *Data Science Journal*, 19(1), 43. doi.org/10.5334/dsj-2020-043.

[5] Waitangi Tribunal. (2011). *Ko Aotearoa Tēnei: Een rapport over claims met betrekking tot Nieuw-Zeelandse wetgeving en beleid die van invloed zijn op Māori cultuur en -identiteit (WAI 262).* Legislation Direct, Wellington.

[6] Europese Commissie. (2024). *Verordening (EU) 2024/1689 van het Europees Parlement en de Raad van 13 juni 2024 tot vaststelling van geharmoniseerde regels inzake kunstmatige intelligentie (Wet inzake kunstmatige intelligentie).*

[7] Europese Commissie. (2024). *Verordening (EU) 2024/1083 van het Europees Parlement en de Raad van 11 april 2024 tot vaststelling van een gemeenschappelijk kader voor mediadiensten in de interne markt (Europese Wet inzake mediavrijheid).*

[8] Europees Parlement en Raad. (2016). *Verordening (EU) 2016/679 (Algemene Verordening Gegevensbescherming),* artikelen 9, 15, 16, 17, 18, 20, 21.

[9] Amerikaans Congres. (2018). *Clarifying Lawful Overseas Use of Data Act (CLOUD Act),* Pub. L. nr. 115–141, Div. V (23 maart 2018).

[10] European Union Public Licence v1.2 (EUPL-1.2). https://joinup.ec.europa.eu/collection/eupl. Goedgekeurd door de Europese Commissie, 2017.

[11] World Wide Web Consortium. (2022). *Decentralized Identifiers (DIDs) v1.0 — Core Architecture, Data Model, and Representations.* W3C-aanbeveling.

[12] Stroh, J. G. (2026). *Sovereign-Record Architecture for Community-Scale Platforms — A Phase 1 Implementation Report, v0.4.* My Digital Sovereignty Limited (NZ). Voorafgaand concept van dit document; bewaard als historisch document van de architectuurstatus van fase 1.

[13] Radio New Zealand / 1News. (februari 2026). *MFAT bevestigt besprekingen over een Enhanced Border Security Partnership met de Verenigde Staten.* Officiële verklaring van het Ministerie van Buitenlandse Zaken en Handel.

[13a] Waitangi Tribunal. *Onderzoek WAI 2522.* Twee eindrapporten die relevant zijn voor dit document: (i) *Rapport over de Trans-Pacific Partnership Agreement* (2016); (ii) *Het rapport over de Comprehensive and Progressive Agreement for Trans-Pacific Partnership* (2021). Een derde rapport in het kader van hetzelfde WAI 2522-onderzoek — *Rapport over de herziening door de Kroon van het stelsel van kwekersrechten* (2020) — is verwant maar wordt hier niet aangehaald. Alle rapporten zijn beschikbaar op waitangitribunal.govt.nz.

[14] Centrist.nz. (2026). *Grensbeveiligingsovereenkomst tussen Nieuw-Zeeland en de Verenigde Staten: stand van zaken bij de onderhandelingen.* Geraadpleegd via de berichtgeving van centrist.nz over de EBSP-besprekingen.

[15] Oceanic Press. (2026). *EBSP-besprekingen: ambtenaren bevestigen dat er onderhandeld wordt over de reikwijdte en vereisten.*

[16] Privacy Foundation New Zealand. (2026). *Standpuntverklaring over het delen van biometrische gegevens met de Verenigde Staten in het kader van het Enhanced Border Security Partnership.* Persbericht van Privacy Foundation NZ .

[17] Biometric Update. (2026). *Nieuw-Zeeland overweegt toegang van de VS tot biometrische en identiteitsgegevens van burgers in het kader van EBSP-besprekingen.*

[18] Gunasekara, G. (2026). *Analyse van het Enhanced Border Security Partnership en de bepalingen inzake directe toegang tot de database van het DHS.* Juridisch commentaar van de Universiteit van Auckland.

[19] Cochrane, T. (2024). *Moet Nieuw-Zeeland streven naar een uitvoeringsovereenkomst in de stijl van de CLOUD Act? Implicaties voor digitale privacy.* Door de Privacycommissaris gefinancierd onderzoek.

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

[21] Bluesky Public Benefit Corporation. (2024). *AT Protocol specificatie.* https://atproto.com. Accountportabiliteit + gedecentraliseerde identificatie (op DID gebaseerd) handle-resolutie.

[22] Mansour, E., Sambra, A. V., Hawke, S., Zereba, M., Capadisli, S., Ghanem, A., Aboulnaga, A., & Berners-Lee, T. (2016). *Een demonstratie van het Solid-platform voor sociale webtoepassingen.* Bijlage bij de 25e Internationale Conferentie over het World Wide Web. Plus lopend specificatiewerk van de W3C Solid Community Group op https://solidproject.org.

[23] McMahan, H. B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017). *Communicatie-efficiënt leren van diepe netwerken uit gedecentraliseerde gegevens.* In *Artificial Intelligence and Statistics (AISTATS)*. Het oorspronkelijke artikel over federated learning .

[24] Kairouz, P., et al. (2021). *Advances and Open Problems in Federated Learning. Foundations and Trends in Machine Learning*, 14(1-2), 1-210. Uitgebreid overzicht van architecturale keuzes en open problemen bij federated learning.

[25] Walter, M., & Suina, M. (2019). *Inheemse data, inheemse methodologieën en inheemse gegevenssoevereiniteit. International Journal of Social Research Methodology*, 22(3), 233-243.

[25a] Taiuru, K. (3 mei 2026). *AI-agenten en rechtspersoonlijkheid in Nieuw-Zeeland.* `taiuru.co.nz/ai-agents-and-legal-personhood-in-new-zealand/`. Geraadpleegd op 03-05-2026. Persoonlijk opiniestuk (bevat de expliciete disclaimer van de auteur dat hij in persoonlijke hoedanigheid schrijft). Stelt de kwestie van rechtspersoonlijkheid voor als een open vraag, waarbij de beslissing wordt uitgesteld tot collectief werk tussen AI-ontwikkelaars, overheidsinstanties en Māori.

[25b] Taiuru, K. (6 maart 2026). *Kaupapa Māori AI Framework — He Tangata, He Karetao, He Ātārangi.* `taiuru.co.kaupapa` Geraadpleegd op 04-05-2026. AI-kader voor inheemse volkeren gebaseerd op Te Tiriti o Waitangi en UNDRIP; noemt toestemming Māori en gegevenssoevereiniteit over trainingsmateriaal en volledige ketenverantwoordelijkheid bij ontwikkelaars, exploitanten en implementators als vereiste praktijk.

[22b] Symmetry Systems. (2024). *Securing Your Sovereign Data+AI Stack.*

Sectoranalyse van soevereine AI-architectuur.

[23b] Merit Data Tech. *Zero-Egress AI: Architecting On-Premise Situated Language Models for Verifiable Data Sovereignty.* Sectoranalyse. [24b] Enterprise DB. Sovereign AI: Ensuring Data and AI

[24b] Enterprise DB. *Soevereine AI: het waarborgen van gegevens- en AI-soevereiniteit in ondernemingen.*

[26] Wachter, S., Mittelstadt, B., & Floridi, L. (2017). *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation.* International Data Privacy Law, 7(2), 76–99. DOI: 10.1093/idpl/ipx005. Geciteerd in §3.5.

[27] Edwards, L., & Veale, M. (2017). *Slave to the Algorithm? Why a 'Right to an Explanation' is Probably Not the Remedy You Are Looking For.* Duke Law & Technology Review, 16(1), 18–84. Beschikbaar op scholarship.law.duke.edu/dltr/vol16/iss1/2. Geciteerd in §3.5.

[28] Te Mana Raraunga (Māori Data Sovereignty Network). (2018, oktober). *Principles of Māori Data Sovereignty.* Opgehaald van temanararaunga.maori.nz/principles-of-maori-data-sovereignty. Geciteerd in §3.6.

[29] Carroll, S. R., Rodriguez-Lonebear, D., & Martinez, A. (2019). *Indigenous Data Governance: Strategies from United States Native Nations.* Data Science Journal, 18, 31. DOI: 10.5334/dsj-2019-031. Geciteerd in §3.6.

[30] Hudson, M., Anderson, T., Dewes, T. K., Temara, P., Whaanga, H., & Roa, T. (2017). *"He Matapihi ki te Mana Raraunga" — Conceptualising Big Data through a Māori lens.* Beschikbaar via Research Commons, Universiteit van Waikato. Geciteerd in §3.6.

[31] Raman, A., Joglekar, S., De Cristofaro, E., Sastry, N., & Tyson, G. (2019). *Uitdagingen in het gedecentraliseerde web: het Mastodon- geval.* In Proceedings of the Internet Measurement Conference 2019 (IMC '19), Amsterdam, oktober 2019. Empirische karakterisering van de Mastodon-federatiegrafiek, instantieconcentratie en operationele kwetsbaarheid onder moderatie op instantieniveau.

[32] Zignani, M., Gaito, S., & Rossi, G. P. (2018). *Volg de "Mastodon": Structuur en evolutie van een gedecentraliseerd online sociaal netwerk.* In Proceedings of the Twelfth International AAAI Conference on Web and Social Media (ICWSM 2018), Stanford, juni 2018. Structurele analyse van het vroege Mastodon-netwerk, inclusief clustering op instanceniveau en eigenschappen van de federatiegrafiek.

[33] Open Data Institute. (oktober 2018). *Defining a "data trust".* ODI Working Paper. Stelt de werkdefinitie van een datatrust vast als "een juridische structuur die onafhankelijk beheer van data biedt", gebruikt in latere Britse overheids- en beleidsliteratuur over het institutionele ontwerp van databeheer.

[34] Element AI / Nesta. (2019). *Data Trusts: A new tool for data governance.* Gezamenlijk gepubliceerd onderzoek naar institutioneel ontwerp van data trusts als mechanisme om machtsongelijkheid tussen technologiebedrijven, de overheid en het publiek aan te pakken.

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

Voorgestelde bronvermelding (na goedkeuring door de beheerder): Stroh, J. G. (2026). *Sovereign-Record Architecture for Community-Scale Platforms — Paper A.* My Digital Sovereignty Limited. (Zenodo DOI wordt toegewezen bij publicatie.)

Conceptstatus: Beoordelingsconcept v4 — mei 2026. Opmerkingen en correcties zijn welkom. Gebaseerd op het voorgaande v0.4 implementatierapport. Structuur voegt Related Work, Threat Model en Evaluation toe volgens stap C van het herpositioneringsplan van 01-05-2026. Begeleidend artikel (Paper B — Situated Language Layers, samenvatting van het empirische begeleidende artikel, gepubliceerd). Gepubliceerd op agenticgovernance.digital als revisieontwerp; Zenodo DOI wordt toegewezen in de v4 release-candidate-fase.