Sovereign-Record-Architektur für Plattformen auf Gemeindeebene

John G. Stroh

Papier A · Entwurf zur Überprüfung v4, Mai 2026 | Sprachen: EN · DE · MI

HTML lesen PDF herunterladen Diashow anzeigen Feedback per E-Mail

Inhaltliches Feedback zu bestimmten Abschnitten ist willkommen. Bitte geben Sie die Abschnittsnummern an (z. B. §6.10), damit Korrekturen nachverfolgt werden können. Der Autor antwortet persönlich; rechnen Sie mit ein bis zwei Wochen. Das Papier ist auf Englisch, Te Reo Māori und Deutsch verfügbar (Links oben). Die Präsentation ist derzeit nur auf Englisch verfügbar; lokalisierte Präsentationen folgen bei der v4-Release-Candidate-Phase.

Sovereign-Record-Architektur für Community-Scale- Plattformen

Kryptografische Herkunftsnachweise, mandantengebundene Durchsetzung von Richtlinien, bilaterale Föderation und mitgliederorientierte souveräne Portabilität für Community-Infrastrukturen ohne Hyperscaler

John G. Stroh

03.05.2026

Sovereign-Record Architektur für Plattformen auf Community-Ebene

Zusammenfassung

Die Standardplattform auf Community-Ebene gehört einem US-Unternehmen, wird auf einer von den USA kontrollierten Infrastruktur gehostet, monetarisiert sich durch die Gewinnung von Aufmerksamkeit und unterliegt Bedingungen, die der Betreiber einseitig ändern kann. Die Allgegenwärtigkeit dieser Standardplattform ist kein wertorientierter Konsens, den Gemeinschaften nach Abwägung von Alternativen erzielt haben; sie ist die Folge von mehr als einem Jahrzehnt anhaltender Unternehmensinvestitionen in die Gestaltung von Nutzererwartungen, in Mechanismen zur Bindung durch Netzwerkeffekte und in die Gestaltung des öffentlichen Diskurses, durch die Alternativen als unpraktisch oder unsichtbar dargestellt werden. Diese Bedingungen bleiben ungeachtet der Zustimmung der Gemeinschaften ununterbrochen in Kraft und treten nur sporadisch als sichtbare Ausfälle zutage – ein gesperrtes Konto, ein gelöschter Beitrag, ein ohne Vorankündigung eingestellter Dienst, eine gegen die Interessen der Gemeinschaft gerichtete Änderung der Nutzungsbedingungen. Für einige Gemeinschaften – Māori-Gemeinschaften, die Taonga bewahren, Minderheitensprachgemeinschaften, deren Inhalt die Sprache selbst *ist*, Familiengeschichtsgruppen, die Aufzeichnungen über namentlich genannte lebende Personen führen, und jede Gemeinschaft, deren Lebensform sich nicht auf ein Profilobjekt reduzieren lässt – sind diese Bedingungen keine erträglichen Unannehmlichkeiten; sie sind strukturelle Hindernisse für die Arbeit, für die die Gemeinschaft existiert. Dieser Beitrag beschreibt eine **Sovereign-Record-Architektur** – eine alternative Grundlage, in der die Souveränitätsgarantien, die eine Gemeinschaft benötigt, Eigenschaften der Datensätze selbst sind und keine Zugeständnisse, die der Betreiber wieder widerrufen kann.

Jeder Inhaltsdatensatz im System trägt seine eigene Provenienz, seine eigene Zugriffsrichtlinie, seine eigene Verschlüsselungskennung und eine kryptografische Kette aller Governance-Grenzen, die er überschritten hat. Lesevorgänge legen diesen Zustand für Verbraucher offen; Schreibvorgänge fügen ihm etwas hinzu; Löschvorgänge markieren ihn als veraltet. Die Föderation zwischen souveränen Mandanten ist bilateral und begrenzt – zwei Gemeinschaften vereinbaren zu von ihnen festgelegten Bedingungen eine bestimmte Interaktion, und nur diese. Mitglieder sind erstklassige betroffene Personen unter dem jeweiligen für sie geltenden Regulierungsrahmen: Jeder kann den vollständigen Satz der Datensätze, in denen er erscheint, in kryptografisch überprüfbarer Form exportieren und zu jedem Mandanten migrieren, der unter demselben Architekturmodell operiert. Eine überwachte Dialogschnittstelle – eine vom Betreiber freigegebene redaktionelle Warteschlange, eine „Entwurf-und-Veröffentlichung“-Sperre, keine automatische Veröffentlichung, keine nach außen gerichtete Kommunikation – erweitert die schreibgeschützte Governance-Benutzeroberfläche für Stakeholder zu einer partizipativen Governance, ohne

die Disziplin der Aufsicht aufzugeben.

Die Architektur läuft in der Produktion auf einer Infrastruktur unter EU-Hoheit (OVH France) und neuseeländischer Hoheit (Catalyst Cloud). Eine Carpool-Konfiguration befindet sich als erste geplante Multi-Instanz-Föderationsbereitstellung im Aufbau. Die bilaterale Verbundinfrastruktur wird End-to-End mit einer umfassenden Negativtestmatrix ausgeliefert, die bereichsgebundene Lesezugriffe, das Blockieren von mandantenübergreifenden Schreibvorgängen, die Vollständigkeit der Audit-Protokolle, die Zitierdisziplin, das Caching-/Veraltungsverhalten, Datenzustände in Randfällen, die Durchsetzung von Autorisierungsgrenzen sowie die Auflösung von Namensraumkonflikten abdeckt; Live-Verbundverbindungen zwischen unabhängigen Mandanten stehen noch aus, bis die erste Multi-Instanz-Carpool-Aktivierung erfolgt.

Die Architektur ist darauf ausgelegt, die Te-Tiriti-Governance-Pflichten in Bezug auf KI-Systeme, die Māori-Daten verwenden oder erzeugen, im Einklang mit den vorgeschriebenen Prinzipien von Dr. Taiurus Kaupapa-Māori-KI-Framework [25b] (Zustimmung der Māori + Datenhoheit über Trainingsmaterial + lückenlose Rechenschaftspflicht). Die offenere Frage, die Dr. Taiuru [25a] hinsichtlich der Rechtspersönlichkeit von KI-Agenten stellt, die auf Māori-Wissen basieren, gehört zum empirischen Bereich des Begleitartikels (Artikel B – Situated Language Layers, Zusammenfassung des empirischen Begleitartikels, veröffentlicht) und wird dort behandelt, nicht in diesem Artikel. Ein Entwicklungszeit-Framework (Tractatus, Apache 2.0) dokumentiert die architektonischen Konsultationen, aus denen dieses Design hervorgegangen ist; das persistente Ledger bildet einen Teil der Evaluierungsfläche. Das Substrat wird von einem kleinen Team in Neuseeland ohne Risikokapital aufgebaut. Es ist eine architektonische Antwort auf die Frage, wie Gemeinschaftsinfrastruktur die Bedingungen der durch US-Plattformen vorgegebenen Souveränität ablehnt, ohne sich von der Arbeit zurückzuziehen, die diese Infrastruktur für die Gemeinschaften leistet, denen sie dient.

Schlüsselwörter: Datenhoheit, Mandantenisolierung, kryptografische Provenienz, bilaterale Föderation, Rechte betroffener Personen, souveräne Portabilität, Te Tiriti o Waitangi, KI-Personenstatus, Kaitiakitanga, Politikvererbung, EUPL-1.2, CARE-Prinzipien, DSGVO Artikel 15, Enhanced Border Security Partnership, CLOUD Act, dezentrale Identifikatoren.

---

1. Einleitung

Die Standardplattform auf Community-Ebene ist eine SaaS-Instanz, die einem US-amerikanischen Unternehmen gehört, auf einer von den USA kontrollierten Infrastruktur gehostet wird, durch Aufmerksamkeitsgewinnung monetarisiert wird und durch Bedingungen geregelt ist, die der Betreiber einseitig ändern kann. Die Allgegenwärtigkeit dieser Standardplattform ist nicht das Ergebnis einer wertorientierten Einigung, die einzelne Nutzer oder Gemeinschaften nach

Abwägung von Alternativen erzielt haben. Sie ist das Ergebnis von mehr als einem Jahrzehnt anhaltender Unternehmensinvestitionen in die Gestaltung von Nutzererwartungen, in Mechanismen zur Bindung durch Netzwerkeffekte und in die Rahmenbedingungen, durch die alternative Arrangements als unpraktisch oder unsichtbar dargestellt werden. Die Bedingungen bleiben ungeachtet der Zustimmung der Gemeinschaft ununterbrochen in Kraft und treten nur sporadisch als sichtbare Ausfälle zutage – ein gesperrtes Konto, ein gelöschter Beitrag, eine ohne Vorankündigung eingestellte Dienstleistung, eine Änderung der Nutzungsbedingungen gegen das Interesse der Gemeinschaft –, während die zugrunde liegende Vereinbarung ununterbrochen in Kraft bleibt. Für manche Gemeinschaften – Māori-Gemeinschaften, die unter den Verpflichtungen des Te Tiriti stehen, Berufsverbände, deren Mitglieder vertrauliches Material besitzen, Familiengeschichtsgruppen, die Aufzeichnungen über namentlich genannte lebende Personen führen, Naturschutzgruppen, deren Standortdaten sensibel sind, Pfarrgemeinden, Sportverbände, Minderheitensprachgemeinschaften und andere, deren Lebensform sich nicht auf ein Profilobjekt reduzieren lässt — sind die zugrunde liegenden Bedingungen unerträglich: Sie stellen strukturelle Hindernisse für die Arbeit dar, zu deren Erfüllung die Gemeinschaft existiert.

Dieser Beitrag richtet sich an diese Gemeinschaften – und an die breitere Gruppe kleiner Organisationen, für die sie beispielhaft stehen: Organisationen, die vertrauliche Informationen über Infrastruktur außerhalb ihres Zuständigkeitsbereichs besitzen, zu Bedingungen, die nur der Betreiber ändern kann.

Auf diese Gemeinschaften wirken drei Druckfaktoren zusammen.

Der erste ist **jurisdiktioneller Natur**. Der CLOUD Act (2018) [9] erweitert die Befugnisse der US-Justizbehörden auf US-amerikanische Cloud-Anbieter weltweit, unabhängig davon, wo die betroffene Person lebt. Die Verhandlungen über die Enhanced Border Security Partnership (EBSP), die derzeit im neuseeländischen Kontext öffentlich diskutiert werden [13][14], sind an die fortgesetzte Teilnahme am US-Visa-Waiver-Programm geknüpft, wobei für die verhandelnden Länder eine Frist gesetzt wurde [13][14][15], und sehen einen erweiterten Datenzugriff einschließlich biometrischer und anderer Identitätsdaten vor [16][17]. Ein juristischer Kommentar der Universität Auckland [18] stellt fest, dass die Unterlagen des US-Ministeriums für Innere Sicherheit beschreiben, dass die EBSP-Vereinbarungen deutlich über die fallbezogenen Übermittlungen im Rahmen bestehender Passenger Name Record (PNR)-Abkommen hinausgehen, was die Aussicht auf direkten Datenbankzugriff eröffnet. Die Privacy Foundation New Zealand hat Bedenken hinsichtlich Transparenz und Schutzmaßnahmen geäußert [19]. Souveränität ist in diesem Zusammenhang kein Marketingbegriff: Es geht darum, welcher Staat die Offenlegung erzwingen kann, nach welchem Zeitplan und mit welcher Benachrichtigung an die Gemeinschaft, deren Daten offengelegt werden.

Der zweite Aspekt ist **regulatorischer Natur**. Te Tiriti o Waitangi (der Vertrag von 1840 zwischen der Krone und den Māori), das EU-KI-Gesetz [6], die Artikel 9 und 15 der DSGVO [8] sowie das Europäische Gesetz zur

Medienfreiheit [7] erlegen der Dateninfrastruktur der Community jeweils Verpflichtungen auf, die durch Delegation nur schwer oder gar nicht zu erfüllen sind. Ein Plattformbetreiber, der nicht nachweisen kann, welches Modell die Inhalte welches Mitglieds anhand welcher von der Gemeinschaft verfassten Richtlinien und mit welcher Entscheidung bewertet hat, kann die in diesen Instrumenten genannten Verpflichtungen nicht erfüllen. Eine Plattform, die einem Mitglied auf Anfrage nicht den vollständigen Satz der von ihm verfassten Datensätze in überprüfbarer Form zur Verfügung stellen kann, kann das Auskunftsrecht gemäß Artikel 15 der DSGVO nicht erfüllen. Gemeinschaften, die unter Te Tiriti operieren, unterliegen einer entsprechenden Verpflichtung gemäß Artikel 2 – Rangatiratanga über Taonga –, die eine Architektur strukturell unterstützen muss, anstatt sie nur zu deklarieren.

Der dritte Punkt ist **technischer Natur**. Der handelsübliche KI-Stack leitet Inferenzprozesse über eine kleine Anzahl von US-Infrastrukturanbietern und behandelt die Inhalte jeder Gemeinschaft als potenziellen Trainingsinput. Für Gemeinschaften, deren Vokabular, Governance-Protokolle oder heilige Materialien nicht ohne Schaden in einen globalen Korpus einfließen können – und deren Verpflichtungen aus Te Tiriti oder den CARE-Prinzipien durch eine solche Durchschnittsbildung verletzt würden –, ist der handelsübliche Stack unbrauchbar.

Dieser Beitrag stellt eine architektonische Lösung vor. Das zentrale Versprechen ist konkret: Jeder Inhaltsdatensatz trägt seine eigene Herkunft, seine eigene Zugriffsrichtlinie und eine kryptografische Kette aller Governance-Grenzen, die er überschritten hat. Lesevorgänge legen diesen Status für Verbraucher offen; Schreibvorgänge fügen ihn an; Löschvorgänge markieren ihn als veraltet. Die Architektur läuft in der Produktion über mehrere dorfartige Konfigurationen hinweg auf Infrastruktur unter der Hoheit der EU und Neuseelands. Die Arbeit wurde ohne Risikokapital, mit dem Budget eines kleinen Teams, von einem privaten neuseeländischen Unternehmen durchgeführt, unter Verwendung eines Governance-Frameworks für die Entwicklungsphase (Tractatus), das seine eigenen architektonischen Entscheidungen im Laufe des Prozesses aufzeichnet.

Der Artikel ist wie folgt aufgebaut. §2 legt den Hintergrund dar – das Governance-Framework für die Entwicklungsphase, den Rahmen von Te Tiriti und den CARE-Prinzipien für indigene Datenhoheit (mit Dr. Taiurus (2026) Zwei-Register-Argument zu den Te-Tiriti-Verpflichtungen und die offene Frage der Rechtspersönlichkeit von KI-Agenten, die in §3.6 erörtert wird), die operative Definition *souveräner Datensätze*, den bilateralen Rahmen der Föderation und den Rahmen „Mitglied als Datensubjekt“ für souveräne Portabilität. §3 positioniert die Arbeit im Vergleich zur einschlägigen Literatur, einschließlich der Auseinandersetzung mit Dr. Taiurus Argument als zitierte veröffentlichte Arbeit. §4 formalisiert das Bedrohungsmodell mit benannten Angreifern und überprüfbaren Prädikaten. §5 legt die Entwurfsprinzipien dar. §6 berichtet über die architektonische Umsetzung. §7 berichtet über die Föderation in der Produktion. §8 berichtet über souveräne Portabilität. §9

berichtet über die Stakeholder-Governance-Benutzeroberfläche, einschließlich der ausgelieferten Phase-6-Oberfläche für den überwachten partizipativen Dialog. §10 führt ein Anwendungsbeispiel für den domänenübergreifenden Transfer der Namenshoheit zwischen zwei situierten Sprachmodulen durch. §11 gibt einen Überblick über die „Village“-Konfigurationen. §12 berichtet über die Evaluierung. §13 beschreibt die Open-Source-Strategie. §14 legt den architektonischen Beitrag dar. §15 nennt, was die Architektur noch nicht leistet.

---

2. Hintergrund

2.1 Das Tractatus-Framework

Die Governance-Mechanismen, die während der Entwicklungsphase zum Aufbau und Betrieb der Plattform verwendet wurden, sind das Tractatus-Framework, ein separates Forschungsprojekt desselben Autors. Das Framework umfasst eine Reihe von Architekturmustern und Code-Diensten für die KI-Governance während der Entwicklung – hauptsächlich Dienste, die an architektonischen Entscheidungspunkten in die Entscheidungsfindung eines KI-Codierungsassistenten eingreifen. Das Framework ist Open Source unter der Apache 2.0-Lizenz und wird öffentlich unter `codeberg.org/mysovereignty/tractatus-framework` [1] bereitgestellt. Ein Arbeitspapier dokumentiert die Beobachtungsergebnisse des Frameworks und die darin kodifizierten Architekturmuster; konkrete quantitative Zahlen werden im Arbeitspapier aufgeführt und nicht hier erneut aufgeführt.

Tractatus ist Governance *in der Entwicklungsphase*: Es prägt den Quellcode und die architektonischen Entscheidungen der Plattform, nicht deren Laufzeitanfragen. Die Plattform konsultiert das Framework an architektonischen Entscheidungspunkten und speichert jede Konsultation als Datensatz in der Plattformdatenbank; Konsultationen werden nach Revisionskennung, Dienst, Bedingungsliste und PASS/FAIL-Urteil gespeichert. Die Disziplin der Aufzeichnung der Konsultation – einheitlich in lokalen sowie in EU- und neuseeländischen Produktionsdatenbanken, automatisiert durch Skripte pro Entscheidung – ist der Beitrag; ein zukünftiger Leser kann fragen, welche Bedingungen eine bestimmte architektonische Entscheidung betraf, und die Antwort findet sich in der Datenbank, nicht im Text.

Diese Trennung ist wichtig. Tractatus ist das Framework. Die Plattform ist eine Anwendung davon. Dieser Artikel berichtet über die Plattform; das Framework wird der Vollständigkeit halber genannt, da die Codebasis der Plattform es an jedem architektonischen Entscheidungspunkt konsultiert.

2.2 Te Tiriti o Waitangi und indigene Datenhoheit

Te Tiriti o Waitangi, der Vertrag von 1840 zwischen der britischen Krone und den Māori-Stämmen, bildet die Grundlage des neuseeländischen Verfassungsrechts. Seine drei Artikel – die Anerkennung der Souveränität der Stämme über Taonga (geschätzte Gegenstände), die Regierungsgewalt der Krone und die Gleichberechtigung der Bürger – bilden den Rahmen für die heutigen Verpflichtungen im Bereich Daten. Der Bericht *WAI 262* des Waitangi-Tribunals [5] und die *CARE-Prinzipien für indigene Daten Governance* [4] sind viel zitierte Formulierungen dessen, was diese Verpflichtungen für die Dateninfrastruktur von Gemeinschaften bedeuten. Die CARE-Prinzipien – Kollektiver Nutzen, Kontrollbefugnis, Verantwortung, Ethik – sind nicht mit den FAIR-Prinzipien für offene Daten identisch; sie bestehen neben diesen und haben ausdrücklich Vorrang, wenn es zu Widersprüchen zwischen beiden kommt.

Ein neuerer Bericht des Tribunals, *WAI 2522* [13a], erweiterte die Analyse auf internationale Wirtschaftsinstrumente – die Untersuchung zur Transpazifischen Partnerschaft, das Mediationsabkommen und die Umsetzung dieser Instrumente durch das Ministerium für auswärtige Angelegenheiten und Handel. Die Schlussfolgerungen des Tribunals in WAI 2522 sowie die Arbeit von Ngā Toki Whakarururanga als Instrument für die Zusammenarbeit zwischen Māori und Krone schärfen die Verpflichtung: Eine Krone, die Māori-Daten einem ausländischen Rechtssystem aussetzt – durch Datenlokalisierungsverbote in Handelsabkommen, durch Exposition durch den CLOUD Act, durch eine „Enhanced Border Security Partnership“, die direkten Datenbankzugriff vorsieht – kann den Schutz von Taonga gemäß Artikel 2 nicht erfüllen, es sei denn, die Architektur selbst verhindert eine solche Exposition. Architektonische Souveränität ist die einzige Souveränität, die der Prüfung gemäß Artikel 2 standhält, sobald die eigenen Vertragspflichten der Krone Exportwege schaffen.

Für Māori-Gemeinschaften, die ihre Rechte gemäß Te Tiriti geltend machen, muss eine Gemeinschaftsplattform es ihnen ermöglichen, ihre Daten auf einer Infrastruktur zu speichern, die sie überprüfen können, die gemäß ihren Tikanga (gewohnheitsrechtlichen Protokollen) verwaltet wird und die keinen gemeinschaftsübergreifenden Zugriff zulässt – auch nicht durch den Plattformbetreiber. Die Architektur gibt darauf eine direkte Antwort: Die Isolierung der Mandanten ist das grundlegende Element, keine Funktion. Ein Plattformbetreiber mit Zugriff auf Tenant-Daten auf Inhaltsebene kann die Verpflichtung der CARE-Prinzipien *zur Kontrollhoheit* nicht erfüllen.

Dr. Karaitiana Taiuru (Ngāi Tahu, Ngāti Kahungunu) hat umfangreich zu Māori-Technologieethik, indigener Datenhoheit, KI-Ethik und digitalen Rechten veröffentlicht; seine Arbeiten sind unter taiuru.co.nz verfügbar. Die auf der hier beschriebenen Plattform laufende, ortsspezifische Sprachschicht wurde auf der Grundlage von Dr. Taiurus veröffentlichten Rahmenwerken mit seiner Genehmigung und unter Angabe der Quelle trainiert. Dr. Taiurus

umfassenderes Werk zur KI-Governance der Māori ist der feste Bezugspunkt für die Position dieses Artikels. Sein Kaupapa Māori AI Framework [25b] (März 2026), ausgedrückt im Whakatauāki *He Tangata, He Karetao, He Ātārangi* (ein Mensch, eine Marionette, ein Schatten), benannt, nennt die Zustimmung der Māori und die Datenhoheit über das im KI-Training verwendete Wissen sowie die lückenlose Rechenschaftspflicht über Entwickler, Betreiber und Implementierer als erforderliche Praxis, die auf dem Te Tiriti und der UN Erklärung der Vereinten Nationen über die Rechte indigener Völker. Die in diesem Beitrag beschriebenen architektonischen Grundelemente sind darauf ausgelegt, diese vorgeschriebenen Praktiken umzusetzen. Dr. Taiurus jüngere Untersuchung [25a] wirft separat die offene Frage auf, ob und unter welchen Bedingungen die Rechtspersönlichkeit auf KI-Agenten ausgeweitet werden könnte, die auf Māori-Wissen basieren – unter Berufung auf die Feststellung der WAI 2522, dass Māori-Daten „taonga“ sind, und auf den Präzedenzfall der drei Gesetze zur Rechtspersönlichkeit natürlicher Merkmale (Te Urewera 2014; Te Awa Tupua 2017; Te Kāhui Tupua 2025) – eine Untersuchung, die er ausdrücklich der gemeinsamen Arbeit von KI-Entwicklern, Regierungsbehörden und Māori-Gemeinschaften überlässt. Die Untersuchung zur Rechtspersönlichkeit gehört zum empirischen Bereich des Begleitpapiers B (Zusammenfassung des empirischen Begleitpapiers, veröffentlicht), in dem das Architekturmuster der situierten Sprachebene und die Funktionsprinzipien beschrieben werden und in dem das vollständige empirische Papier detailliert über die Ausbildungsdisziplin der Kohorte berichten wird, auf die sich jede zukünftige partnerschaftliche Zusammenarbeit pro Kohorte (einschließlich Meads Tikanga-Test) stützen würde; dieses Papier greift dieser Arbeit nicht vor.

Die Architektur geht nicht speziell von Māori-Gemeinschaften aus. Die gleiche Eigenschaft – eine Plattform, die nicht gemeinschaftsübergreifend sehen kann – entspricht den regulatorischen Verpflichtungen, denen Minderheitensprachen-Gemeinschaften in der EU gemäß dem Europäischen Medienfreiheitsgesetz und den Schutzbestimmungen für besondere Kategorien in Artikel 9 der DSGVO unterliegen, wobei kulturelle Daten von Minderheitensprachen plausibel als besondere Kategorie ausgelegt werden. Eine walisische Gemeinschaft, eine samische Gemeinschaft, eine sorbische Gemeinschaft, eine friesische Gemeinschaft, eine katalanische Gemeinschaft kann dieselbe Architektur übernehmen, indem sie die Sprachschicht auf einem anderen Korpus neu trainiert und die Richtlinie unter ihrem eigenen Rechtsrahmen neu formuliert; die Architektur selbst ist portabel. Diese Portabilität ist eine zentrale architektonische Eigenschaft.

2.3 Warum „souveräne Datensätze“ statt „verschlüsselt im Ruhezustand“

Der Begriff *„souveräner Datensatz“* ist bewusst gewählt. Verschlüsselung im Ruhezustand ist eine Funktion; Souveränität ist eine architektonische

Eigenschaft. Ein Datensatz ist in dem hier beabsichtigten Sinne souverän, wenn alle folgenden Bedingungen zutreffen:

1. Es trägt seine eigene Herkunft – wer es verfasst hat, wer sein Kaitiaki (Verwalter) ist, unter welchen Tikanga es geteilt wurde, wann es erstellt wurde und einen kryptografischen Hash, der diese Felder miteinander verknüpft.
2. Es trägt seine eigene Richtlinie in sich – wer es lesen darf, wer damit trainieren darf, wer es exportieren darf, was passiert, wenn Richtlinien miteinander in Konflikt stehen.
3. Es verfügt über eine eigene Proof-Chain – jede Governance-Grenze, die es überschritten hat (Erstellung, Aktualisierung, Export, Löschung), wird mit einer kryptografischen Signatur aufgezeichnet.
4. Der Cache seines Verifizierungsstatus ist zum Zeitpunkt des Lesens einsehbar – jeder API-Nutzer sieht, ob die Kette des Datensatzes aktuell, abgelaufen, nicht übereinstimmend oder nicht überprüfbar ist, ohne sich auf das Wort der Plattform verlassen zu müssen.
5. Er ist auf Antrag eines Mitglieds übertragbar. Ein Mitglied kann den vollständigen Satz von Datensätzen exportieren, in denen es als Autor, Kaitiaki oder anderweitig als betroffene Person genannt ist; der Export führt die Nachweiskette fort; ein externer Prüfer, der über das veröffentlichte Identifikationsdokument des Quellmandanten verfügt, kann jeden signierten Eintrag in den Datensätzen rekonstruieren.

Dies sind operative Eigenschaften, die über die API-Oberfläche überprüfbar sind, und keine Wunschvorstellungen. Im weiteren Verlauf dieses Papiers wird beschrieben, wie jede dieser Eigenschaften aufgebaut ist.

2.4 Föderation: bilateral und begrenzt

Eine Föderation im Sinne der Plattform ist eine eng gefasste technische Vereinbarung, die es zwei souveränen Mandanteninstanzen ermöglicht, sich für bestimmte, begrenzte Zwecke – gemeinsame Veranstaltungen, gemeinsame Fahrgemeinschaften, instanzübergreifende Ankündigungen – zu verbinden, ohne dabei Daten, Identität oder Governance-Befugnisse abzugeben. Eine Föderation ist eine bilaterale Vereinbarung: Die Verfassungen der beiden Mandanten stimmen überein, die beiden Betreiber stimmen überein, das Föderationsmanifest wird von beiden unterzeichnet. Es gibt keinen zentralen Föderationsserver; der Datenfluss erfolgt direkt, die Governance ist lokal, und jede Partei kann die Föderation jederzeit widerrufen.

Dies unterscheidet sich strukturell vom Plattformmodell, bei dem Instanzen Blätter im Baum eines einzigen Betreibers sind. Es unterscheidet sich auch strukturell vom vorherrschenden Fediverse-Modell, bei dem die Föderation eine netzwerkweite Eigenschaft ist, die durch ein gemeinsames Protokoll zwischen betreibergesteuerten Servern vermittelt wird. Die hier beschriebene Architektur ist bilateral und begrenzt: Zwei Gemeinschaften vereinbaren zu von ihnen

festgelegten Bedingungen eine bestimmte Interaktion und nur diese.

§3 stellt dies der einschlägigen Literatur gegenüber. §7 berichtet über die bereits ausgelieferte Föderationsinfrastruktur und den Status der Live-Bereitstellung. §10 führt ein konkretes Beispiel einer bilateralen Föderation zwischen einem Modul für botanisches Wissen und einem Modul zur Sprachrevitalisierung durch – eine Art von Föderation, die für die Integration in den Lehrplan von Grundschulen in Betracht gezogen wird.

2.5 Das Mitglied als betroffene Person

Ein Mitglied eines Tenants mit souveränen Datensätzen ist gleichzeitig Mitglied der Community (mit den sozialen, governancebezogenen und inhaltsgestalterischen Rechten, die diese Mitgliedschaft mit sich bringt) und eine betroffene Person im Sinne der für sie geltenden Rechtsrahmen. Ein Mitglied der walisischsprachigen Gemeinschaft ist eine betroffene Person im Sinne der DSGVO; die Daten eines Mitglieds der Māori-Gemeinschaft fallen sowohl unter die Te Tiriti-Rechte des Iwi als auch unter die DSGVO-Rechte des Einzelnen, wenn der Iwi eine in der EU gehostete Infrastruktur für Mitglieder der Diaspora betreibt; ein Mitglied eines deutschen Vereins ist ganz einfach eine betroffene Person im Sinne der DSGVO.

Die Architektur behandelt die Einordnung des Mitglieds als betroffene Person als vorrangig. Der Block `„metadata.origin"` jedes Datensatzes nennt den Autor und (sofern unterschiedlich) den Kaitiaki, beide als dezentrale Identifikatoren. `Der metadata.policy-Block` jedes Datensatzes legt fest, ob und wie dieser Datensatz geteilt, für Trainingszwecke verwendet oder exportiert werden darf, und Konflikte zwischen Richtlinien werden über die verfassungsmäßige Standardeinstellung gelöst. Der mitgliedergesteuerte Export (§8) nimmt die Richtlinie wörtlich: Die Richtlinie eines Datensatzes kann dessen Export sogar durch den Autor selbst verbieten (z. B. bei einer unter Bedingungen der kollektiven Zustimmung eingereichten Beratung), und der Export-Wrapper setzt dies durch. Souveränität ist kein Gegensatz zwischen Mitglied und Kollektiv; sie ist der architektonische Rahmen, innerhalb dessen beide Rechte koexistieren, und dieser Rahmen macht den Konflikt explizit, anstatt ihn in Implementierungsentscheidungen zu verbergen.

---

3. Verwandte Arbeiten

Die Architektur befindet sich an der Schnittstelle mehrerer aktiver Forschungs- und Entwicklungslinien. Diese Positionierung ist entscheidend, da der Beitrag nicht in der Einführung einer einzelnen Primitive besteht – bekannte Bausteine werden wiederverwendet –, sondern in der Integration dieser Primitiven in ein Substrat, das auf das in §4 beschriebene Bedrohungsmodell von der Datensatzebene aufwärts reagiert, anstatt von der Betreiberebene abwärts.

Die in den Abschnitten 3.1–3.7 folgende Literaturübersicht ordnet die Ziele dieses Artikels in den benachbarten Forschungskontext ein. Leser, die sich auf Governance-Argumente konzentrieren, können zu §7 (Föderation in der Produktion), §8 (souveräne Portabilität) oder §9 (Stakeholder-Governance-UI) übergehen, mit der Erkenntnis, dass die Primitive der Architektur – bilaterale Föderation, souveräne Portabilität, kryptografische Löschgarantien, die auch bei einer Kompromittierung des Betreibers bestehen bleiben – zur Laufzeit unabhängig von der Absicht des Betreibers nicht umgangen werden können. Die nachstehende Literaturübersicht zeigt auf, wie sich die einzelnen Primitive im Verhältnis zu ihren nächsten Entsprechungen in der veröffentlichten Forschung verhalten.

3.1 Föderierte soziale Infrastruktur

ActivityPub [Snell & Prodromou, 2018, W3C-Empfehlung [20]] und das Mastodon-Ökosystem etablieren die Föderation als eine netzwerkweite Eigenschaft, die durch ein gemeinsames Protokoll zwischen betreibergesteuerten Servern vermittelt wird. In der ActivityPub-Föderation verbinden sich zwei Server durch den Austausch signierter Aktivitätsobjekte; die Granularität erfolgt pro Akteur und pro Aktivität, vermittelt durch die Sammel-Endpunkte des Protokolls. Dies unterscheidet sich strukturell von der hier beschriebenen bilateralen und begrenzten Föderation. Der Beitrag von ActivityPub ist die Interoperabilität über Tausende von Instanzen hinweg; der Beitrag dieses Artikels ist die Wahrung der Souveränität über jeweils genau zwei Instanzen hinweg, mittels signiertem Manifest, wobei die Widerrufbarkeit als Operation erster Klasse gilt. Beide Architekturen sind gültige Antworten auf unterschiedliche Souveränitätsansätze: ActivityPub ist auf die Reichweite des Graphen optimiert; dieser Artikel ist auf die tribale/kollektive Autorität über den Föderations- Rahmen optimiert.

Die Literatur zu dezentralen sozialen Medien dokumentiert Eigenschaften von Föderationsgraphen, Abwägungen bei der Moderation auf Instanzebene und Lücken bei der Inhaltsportabilität. Empirische Charakterisierungen des Mastodon-Graphen und von Mustern der Instanzmoderation [31][32] fließen in die operative Analyse von Fediverse-Plattformen ein; nachfolgende Arbeiten zum AT-Protokoll [Bluesky Public Benefit Corporation, 2024 [21]] schlugen die Portabilität von Konten vor – die Daten eines Mitglieds folgen dem Mitglied statt dem Server – als strukturelle Antwort auf das Problem der Moderation und Auffindbarkeit. Die in diesem Artikel beschriebene souveräne Portabilität (§8) ist technisch verwandt, aber anders motiviert: Portabilität ist ein Recht der betroffenen Person gemäß Artikel 15 der DSGVO, und die verfassungsrechtliche Akzeptanzprüfung des empfangenden Mandanten (§8) ist integraler Bestandteil, nicht optional. Die Portabilität des AT-Protokolls ist kontobasiert; die Portabilität in diesem Artikel ist datensatzbasiert und rücksichtsvoll gegenüber Richtlinien, mit einem Manifest der Sperrliste, das Datensätze abdeckt, deren Richtlinie den Export selbst durch ihren Autor

verbietet.

3.2 Dezentrale Identifikatoren und überprüfbare Berechtigungsnachweise

Die W3C-Spezifikation „Decentralized Identifiers (DIDs) v1.0“ [11] legt ein methodenunabhängiges Identifikationsschema fest, das mehrere Auflösungsmechanismen unterstützt. Die Mandanten und Mitglieder der Plattform veröffentlichen DID-Dokumente an bekannten Endpunkten unter der eigenen Domain des Mandanten; die Verifizierung kryptografischer Operationen (Provenienz-Hashes, Proof-Chain- Signaturen, Föderationsmanifeste, Export-Bundles) erfolgt anhand dieser Dokumente. Dieses Muster ist weit verbreitet; die architektonische Entscheidung besteht darin, jede kryptografische Operation im System unabhängig überprüfbar zu machen, wobei nur das vom Quell-Mandanten veröffentlichte DID- Dokument und standardmäßige kryptografische Primitive verwendet werden – kein Drittanbieter-Verifizierer, keine gemeinsame Vertrauenswurzel, kein zentralisiertes Register.

3.3 Solid und persönliche Datenspeicher [Mansour et al., 2016 [22]; W3C Solid Community Group] sowie die

Solid [Mansour et al., 2016 [22]; W3C Solid Community Group] und die Inrupt-Plattform speichern Daten in persönlichen Pods, die der betroffenen Person gehören, wobei Anwendungen den Zugriff über eine WebID-basierte Autorisierung anfordern. Das architektonische Ziel von Solid sind *Daten pro Einzelperson*; das Ziel dieses Papiers sind *Daten pro Gemeinschaft, wobei die Mitglieder als vollwertige Datensubjekte innerhalb der Gemeinschaft gelten*. Die beiden Konzeptionen ergänzen sich eher, als dass sie miteinander konkurrieren: Ein Solid-Pod könnte grundsätzlich als Exportziel für ein Sovereign-Record-Bundle dienen, und eine Gemeinschaft, deren Mitglieder jeweils Solid-Pods verwalten, könnte grundsätzlich den Sovereign-Record-Tenant der Plattform darauf implementieren. Die Entscheidung der Plattform, die *Gemeinschaftseinheit* in den Mittelpunkt zu stellen, spiegelt eine grundlegende Position wider, wonach Minderheitensprachen- und indigene Gemeinschaften keine Ansammlungen einzelner Datensubjekte sind: Das Kollektiv ist der Rechteinhaber für Taonga (CARE-Prinzip: Kollektiver Nutzen), und die Architektur muss der Autorität des Kollektivs dienen (Kontrollbefugnis).

3.4 Föderiertes Lernen und Datentreuhandfonds

Federated Learning [McMahan et al., 2017 [23]; Kairouz et al., 2021 Übersichtsartikel [24]] *unterscheidet sich architektonisch* von der vorliegenden Arbeit. Beim Federated Learning wird ein gemeinsames Modell trainiert, indem Gradientenaktualisierungen zwischen den Dateninhabern ausgetauscht werden, ohne dass Rohdaten ausgetauscht werden. Die Föderation in dieser Arbeit tauscht überhaupt keine Modellparameter aus – die Föderation ist eine Datenvereinbarung zwischen Mandanten unter einem signierten Manifest, wobei der Datenfluss pro Vereinbarung definiert ist und kein gemeinsames

Modell impliziert wird. Die situationsbezogene Sprachschicht der Plattform ist konstruktionsbedingt mandantenbezogen; die mandantenübergreifende gemeinsame Nutzung von Modellparametern würde die grundlegende Primitiv der Mandantenisolierung (§5.1) verletzen. Empirische Belege aus der Trainingsdisziplin für die Situated-Language-Schicht werden separat in Paper B dargestellt (Zusammenfassung des empirischen Begleitartikels, veröffentlicht).

Datentreuhandstellen – wie sie in der Arbeitsdefinition des Open Data Institute als „eine rechtliche Struktur, die eine unabhängige Verwaltung von Daten gewährleistet“ [33] und in der parallelen Forschung von Element AI zum institutionellen Design von Datentreuhandstellen als Mechanismus zur Bewältigung von Machtasymmetrien zwischen Technologieunternehmen, Regierung und Öffentlichkeit [34] entwickelt wurden – führen einen externen Treuhänder ein, der Daten im Namen einer Gemeinschaft verwahrt und den Zugriff vermittelt. Die Architektur dieses Artikels kennt keinen solchen Treuhänder. Der Plattformbetreiber kann Infrastrukturvorgänge ausführen (Mandanten anlegen, Abrechnung verwalten, Zustand überwachen), aber keine Mandantendaten einsehen. Es gibt keine Rolle im System, die Daten über mehrere Mandanten hinweg aggregiert, auch nicht vorübergehend. Die Stärke eines Data Trusts liegt in der institutionellen Vermittlung; die Stärke dieser Architektur liegt in der Unmöglichkeit einer Vermittlung von innerhalb der Plattform.

3.5 Umsetzung von Artikel 15/20 der DSGVO Das

Das Recht auf Auskunft (Artikel 15) und das Recht auf Datenübertragbarkeit (Artikel 20) der Datenschutz-Grundverordnung [8] sind Gegenstand einer umfangreichen Literatur zur Umsetzung – darunter Wachter, Mittelstadt & Floridi [26] zur Debatte um das Recht auf Erklärung sowie Edwards & Veale [27], die argumentieren, dass das Recht auf Löschung (Artikel 17) und die Datenübertragbarkeit (Artikel 20) für die algorithmische Rechenschaftspflicht ein größeres praktisches Gewicht haben als das Recht auf Erklärung . Der DSR-Endpunkt der Plattform (§8) implementiert alle sechs relevanten Rechte (Artikel 15, 16, 17, 18, 20, 21) über eine einheitliche Pipeline zum Export souveräner Datensätze, die die Datensätze der betroffenen Person unter vollständiger Wahrung der Proof-Chain in den Formaten JSON, CSV oder PDF-Formaten als ein einziges kanonisches Bündel zurück. Die technische Neuheit hierbei ist die *kryptografische Überprüfbarkeit* des Bündels: Jede externe Partei, die über das veröffentlichte DID-Dokument des Quell-Tenants verfügt, kann jeden Eintrag in den Datensätzen des Bündels überprüfen, ohne entweder dem Quell- Tenant oder dem von der betroffenen Person gewählten Empfänger vertrauen zu müssen. Standardmäßige Artikel-15- Implementierungen geben Daten zurück; diese Implementierung gibt *überprüfbare* Daten zurück.

3.6 CARE Prinzipien und indigene Datenverwaltung

Die CARE-Prinzipien [4] formulieren eine substanzielle Verpflichtung, die architektonische Implikationen hat: *Die Kontrollbefugnis* erfordert, dass die Gemeinschaft – nicht der Plattformbetreiber, nicht ein dritter Treuhänder, nicht eine Regulierungsbehörde mit Vorladungsbefugnis außerhalb der Zuständigkeit der Gemeinschaft – die Daten nach ihren eigenen Bedingungen verwalten kann. Nachfolgende Arbeiten zur indigenen Datenverwaltung – Walter & Suina [25] zu indigenen Daten und Methoden; Te Mana Raraungas *Prinzipien der Māori-Datensouveränität* [28]; Carroll, Rodriguez-Lonebear & Martinez [29] zu Strategien der US-amerikanischen indigenen Nationen; Hudson, Anderson, Dewes, Temara, Whaanga & Roa [30] zur Konzeptualisierung von Big Data aus der Perspektive der Māori – haben die Auswirkungen über den gesamten Datenlebenszyklus (Erhebung, Speicherung, Verarbeitung, Weitergabe, Archivierung) hinweg herausgearbeitet. Die architektonische Entscheidung der Plattform – Tenant-Isolation als Grundlage, souveräne Datensätze als Substrat, bilaterale Föderation als einziger tenantübergreifender Mechanismus – ist eine technische Antwort auf die CARE-Verpflichtungen; sie ist nicht die einzig mögliche Antwort, aber es ist eine architektonische Antwort, die der Prüfung gemäß Artikel 2 des Tiriti im konkreten Fall der Daten neuseeländischer Iwi und dem Druck durch die EBSP-Klasse standhält.

Dr. Taiurus Gesamtwerk zur Māori-KI-Governance [25a, 25b] (vorgestellt in §2.2) konkretisiert die CARE-Verpflichtungen zu spezifischen architektonischen Verpflichtungen. Die präskriptive Pflicht – die Zustimmung der Māori und die Datenhoheit über das im KI-Training verwendete Wissen, lückenlose Rechenschaftspflicht über Entwickler und Betreiber hinweg sowie die Te-Tiriti-Verpflichtungen für KI-Systeme, die Māori-Daten verwenden oder erzeugen – gilt nun für jede Plattform, deren KI-Oberflächen mit Taonga-Material in Berührung kommen. Die in diesem Beitrag beschriebenen architektonischen Grundelemente (Tenant-Isolation als Rangatiratanga gemäß Artikel II über Daten; Tenant-spezifisches Kohorten-Training als Ort des von der Gemeinschaft bestimmten Modellverhaltens für Māori-bezogene Tenants; die ausgelieferte überwachte Dialogschnittstelle der Phase 6 (§9) als Kaitiaki-Aufsicht über das, was die Schnittstelle ausgibt; die Endgültigkeit der kryptografischen Löschung als Rangatiratanga über das, was vergessen wird; DID-basierte Attribution und die Beweiskette als Whakapapa- Rückverfolgbarkeit jedes Datensatzes) sind als strukturelle Antwort auf diese präskriptive Pflicht gedacht. Die weitere Frage, die Dr. Taiuru [25a] aufwirft – ob und unter welchen Bedingungen die Rechtspersönlichkeit auf KI-Agenten ausgeweitet werden könnte, die auf Māori-Wissen basieren, in Anlehnung an die Präzedenzfälle Te Urewera (2014), Te Awa Tupua (2017) und Te Kāhui Tupua (2025) – wird im begleitenden Papier B auf der Ebene der Kohorten-Trainingsdisziplin behandelt und in diesem Papier nicht vorweggenommen.

3.7 Begleitende Bedrohungen: Foreign-Cloud-Mining über Pionier-KI

Branchenkommentare zur Architektur souveräner KI [22b][23b][24b] haben die Konvergenz von US-Rechtsrahmen für den Datenzugriff (CLOUD Act; FISA) und den Einsatz von Frontier-KI-Modellen auf US-kontrollierter Cloud-Infrastruktur als kombinierten Risikoweg analysiert: Daten, auf die unter ausländischem Rechtszwang zugegriffen wird, können von Frontier-KI-Modellen in großem Maßstab nach Mustern durchsucht werden, die über den ursprünglichen Offenlegungsumfang hinausgehen. Die Auswirkungen auf biometrische, Identitäts- und Authentifizierungsdaten sind besonders gravierend. Die architektonische Lösung, die dieser Beitrag vorschlägt, besteht darin, dass kritische Zugangsdaten und biometrische Daten von vornherein niemals in einer aus dem Ausland erreichbaren Cloud-Infrastruktur gespeichert werden und dass jede LLM-Interaktion mit souveränen Daten über eine vom Mandanten verwaltete Schnittstelle läuft, über die der Mandant einschränkt, was ein externes Modell lernen oder speichern darf.

---

4. Bedrohungsmodell

Dieser Abschnitt formalisiert die Bedrohungen, denen die Architektur standhalten soll. Das Modell nennt sechs Angreifer, legt die Souveränitätsinvarianten fest, die jeder von ihnen nicht verletzen darf, und löst jede Invariante in ein überprüfbares Prädikat auf.

4.1 Gegner

A1. Durch Rechtsvorschriften dazu verpflichteter Host-Betreiber. Ein Plattformbetreiber, der selbst durch ein ausländisches Rechtssystem – eine Anordnung nach dem CLOUD Act, einen FISA-Haftbefehl, eine Bestimmung zum Datenbankzugriff im Rahmen der Enhanced Border Security Partnership oder eine gleichwertige Bestimmung unter einer anderen Gerichtsbarkeit – dazu verpflichtet ist, Mandantendaten offenzulegen, auf die er technisch Zugriff hat. Die Verpflichtung kann mit einer Schweigepflichtanordnung einhergehen. Der Betreiber kann in gutem Glauben, in böser Absicht oder unter Zwang handeln; die Architektur ist gegenüber dem Motiv des Betreibers indifferent und geht vom schlimmsten Fall aus. Die Klasse der Angreifer ist nicht hypothetisch: siehe z. B. die Datenpanne bei Instructure / Canvas im Mai 2026, bei der etwa 275 Millionen Datensätze aus 8.809 Bildungseinrichtungen von einem einzigen EdTech-Betreiber abgezogen wurden (mehrere Berichte, darunter Malwarebytes, TechCrunch und SecurityWeek; die Gruppe ShinyHunters bekannte sich zu dem Angriff; Instructure bestätigte den unbefugten Zugriff).

A2. Mitmieter. Ein anderer Mieter auf derselben Plattforminfrastruktur, der versucht, Inhalte zu lesen, die ihm nicht gehören, sei es durch Abfragekonstruktion, Schema-Kenntnisse, Rolleneskalation oder die Ausnutzung einer gemeinsam genutzten Ressource (Datenbank, Cache, Dateisystem).

A3. Peer einer mandantenübergreifenden Föderation. Der Mandant auf der anderen Seite einer bilateralen Föderationsvereinbarung, der versucht, auf Daten außerhalb des im Manifest festgelegten Zwecks zuzugreifen, oder dessen eigene Infrastruktur selbst in Bezug auf die Zuständigkeit kompromittiert ist (Angriff auf die Vertrauenskette über die Föderation).

A4. Mitglied als Angreifer. Ein Mitglied eines Mandanten, das versucht, auf Inhalte zuzugreifen, für deren Lesezugriff es nicht autorisiert ist (z. B. die privaten Beratungen eines anderen Mitglieds, einen auf eine Untergruppe beschränkten Datensatz, derem es nicht angehört), oder das versucht, Befugnisse geltend zu machen, die es nicht besitzt (z. B. eine Mandanten-Admin-Operation durchführen, die Satzung ändern).

A5. Foreign-Cloud-Mining-via-Frontier-AI. Ein Angreifer, der sich über A1 Zugang zu Daten verschafft hat und diese dann durch ein Frontier-AI-Modell leitet, um Muster zu extrahieren, die über den rechtlichen Rahmen der ursprünglichen Offenlegung hinausgehen – biometrische Korrelationen über Bevölkerungsgruppen hinweg, Ableitung von Authentifizierungsmustern aus Sitzungsmetadaten, Rekonstruktion sozialer Netzwerke anhand von Interaktionsspuren.

A6. Angreifer, der biometrische Daten nutzt. Ein Angreifer, der durch die Kombination von A1 (juristisch erzwungener Host) und A5 (Foreign-Cloud-Mining-via-Frontier-AI) versucht, biometrische Daten auszunutzen, die von der Plattform gespeichert werden – Gesichter, Fingerabdrücke, Stimmabdrücke, Iris-Scans, verhaltensbiometrische Profile –, um Mitglieder zu identifizieren, zu korrelieren oder zu erpressen. Der Einfluss des Angreifers wächst mit der Unwiderruflichkeit biometrischer Daten: Ein durchgesickertes Passwort kann geändert werden, ein durchgesickerter Gesichtsabdruck nicht. Die Reichweite des Angreifers wird durch die drei zusammenlaufenden Expositionswege für biometrische Daten im US-Rechtsraum verstärkt – direkte Erfassung auf US-Seite an Grenzen und bei Visumsgesprächen, Hosting in US-Clouds unter dem Zwang des CLOUD Act sowie künftige Vereinbarungen im Rahmen der Enhanced Border Security Partnership, die einen direkten Datenbankzugriff auf biometrische Repositorien von Partnerländern vorsehen. Die architektonische Antwort lautet, dass die Plattform keinerlei biometrische Daten auf irgendeinem von ihr kontrollierten Pfad speichert (siehe §5 Entwurfsprinzipien und §13.1 Anbieterdisziplin).

A7. Fehlzuordnung durch aggregierenden Agenten. Eine zukünftige Agentenoberfläche – laufzeitbasiert, persistent, zielgerichtet –, die Inhalte über Mandanten hinweg oder über Datensätze innerhalb eines Mandanten auf eine Weise aggregiert, die sich `der share_within-Richtlinie` pro Datensatz oder der kaitiaki-Zuordnung pro Datensatz entzieht; oder die emergente Zuordnungen (Urheberschaft, Kaitiakitanga, tikanga-tragende Beziehungen) erzeugt, die die zugrunde liegenden Datensätze nicht rechtfertigen. Die heutige Laufzeitumgebung der Plattform umfasst eine Single-Turn-Verteilung auf der situierten Sprachebene (§5 Entwurfsprinzipien) und die ausgelieferte

partizipative Dialogoberfläche Phase-6 mdsl (§9), die selbst überwacht wird – Single-Turn, vom Betreiber freigegebene redaktionelle Warteschlange, Entwurf-und-Veröffentlichungs-Gate, keine automatische Veröffentlichung, keine nach außen gerichtete Nachrichtenübermittlung. Keines von beiden stellt den vollständigen technischen Mechanismus von A7 dar (Autonomie + Persistenz + datensatzübergreifende Aggregation). Die Te-Tiriti-Governance-Pflicht, die Dr. Taiuru (2026) geltend macht (siehe §3.6), wirkt sich auf die substanzielle Last dieses Gegners aus – nämlich dass jede datensatz- oder mandantenübergreifende Emission eines Māori-tragenden Mandanten diese Pflicht trägt, unabhängig vom Autonomiestufe der Oberfläche. Die bestehende Invariante I3 der Architektur (richtlinienkonforme Offenlegung) ist die primäre technische Verteidigung: Jede datensatz- oder mandantenübergreifende Emission wird an der Routengrenze richtlinienkonform geprüft; die Kaitiaki-Zuordnung und die Beweiskette gewährleisten Whakapapa-Rückverfolgbarkeit durch jeden Datensatz; die Phase-6-Redaktionswarteschlange + das „Draft-and-Publish"-Gate (nach dem Vorbild des Mastodon-Präzedenzfalls „Veröffentlichung nur auf Anweisung") ist die Disziplin gegen das stillschweigende Entstehen von Verhaltensweisen im engeren Sinne aus der überwachten Basislinie. In Anlehnung an Dr. Taiurus umfassenderen Rat – dass die Einhaltung von Tikanga von Anfang an viel einfacher zu integrieren ist als nachträglich – wird A7 hier so benannt, dass jeder zukünftige Schritt in Richtung Autonomie oder Persistenz die Ablehnungseigenschaft als Design-Invariante und nicht als nachträglichen Patch erbt.

4.2 Souveränitätsinvarianten

Für jeden Angreifer verteidigt die Architektur eine oder mehrere Invarianten:

I1. Isolierung von Mandanteninhalten. Keine Plattformbetreiberrolle, kein Mitmandant und kein automatisierter Prozess außerhalb des eigenen Anfragekontexts des Mandanten kann Mandanteninhalte lesen. (Schützt vor A1, A2.)

I2. Authentizität der Herkunft. Der Autor und der Kaitiaki jedes Inhaltsdatensatzes sind kryptografisch an den Inhalt des Datensatzes gebunden; keines der beiden Felder kann stillschweigend geändert werden, ohne den Verifizierungscache ungültig zu machen. (Schützt vor A1, A4.)

I3. Richtlinienkonforme Offenlegung. Jeder mandantenübergreifende oder grenzüberschreitende Datenfluss respektiert die `metadata.policy.share_within` des Datensatzes und den begrenzten Zweck des Verbundmanifests; Flüsse außerhalb dieses Rahmens werden an der Routengrenze abgelehnt. (Schützt vor A1, A3.)

I4. Endgültigkeit der kryptografischen Löschung. Datensätze, bei denen `metadata.policy.delete_must_be_cryptographic` gesetzt ist, sind so löschbar, dass der Chiffretext aus dem persistierten Zustand nicht wiederherstellbar ist, selbst für den Plattformbetreiber mit vollem

Datenbankzugriff. (Schützt vor A1, A5.)

I5. Integrität des Föderationsmanifests. Eine bilaterale Föderation wird erst aktiviert, wenn die Signaturen beider Parteien gegen ihre jeweiligen veröffentlichten DID-Dokumente verifiziert wurden; die Widerrufung ist selbst ein signiertes Ereignis; kein Dritter kann eine Föderation unterlaufen. (Schützt vor A3.)

I6. Nachvollziehbarkeit bei Audits. Jedes grenzüberschreitende Ereignis (Erstellung, Aktualisierung, Export, Löschung, Aktivierung der Föderation, Widerruf der Föderation, Änderung der Mitgliedschaft) hinterlässt einen signierten Eintrag in der Proof-Chain; der Mandant kann jedes Ereignis aus seiner eigenen Datenbank rekonstruieren, ohne sich auf die Angaben des Plattformbetreibers verlassen zu müssen. (Schützt vor A1, A3.)

I7. Ehrlichkeit bei der Souveränitätsportabilität. Der Export der Zugriffsrechte eines Mitglieds wird durch dieselbe Richtlinienkontrolle gefiltert, die auch normale Lesevorgänge regelt; Datensätze, deren Richtlinie den Export verbietet, werden im Exportmanifest als zurückgehalten aufgeführt, wobei der Grund der Richtlinie angegeben wird. (Schützt gegen A4 und sichert die Fähigkeit von A1, zu behaupten: „Wir haben der betroffenen Person alles exportiert, worauf sie Anspruch hatte.“)

I8. Beschränkung des Off-Platform-Mining. Kein Inhaltsdatensatz verlässt die Datenbank des Mandanten in Klartextform, außer über einen Weg, der im Hinblick auf die Satzung des Mandanten überprüft wurde; die Laufzeit-KI- Inferenz (situative Sprachschicht) wird auf mandantengesteuerter Infrastruktur mit richtliniengesteuerter Eingabe ausgeführt. (Schützt vor A5.)

I9. Keine Erfassung biometrischer Daten. Die Plattform erfasst, speichert und verarbeitet keinerlei biometrische Daten auf den von ihr kontrollierten Pfaden – keine Gesichtsabdrücke, keine Fingerabdrücke, keine Stimmabdrücke, keine Irisvorlagen, keine verhaltensbiometrischen Profile, keine aus biometrischen Daten abgeleiteten Schlüssel. (Schützt vor A6; stärkt A1 – der Betreiber kann nicht gezwungen werden, offenzulegen, was nie erfasst wurde; stärkt A5 – es gibt keine biometrische Erfassungsfläche.)

4.3 Überprüfbare Prädikate

Jede Invariante lässt sich auf ein oder mehrere Prädikate zurückführen, die über die API-Oberfläche oder durch direkte Datenbankprüfung testbar sind.

Für I1 (Isolierung von Mandanteninhalten): Alle Abfragen für mandantenbezogene Datensammlungen sind so aufgebaut, dass das Weglassen eines Mandantenfilters einen Laufzeitfehler auslöst; eine automatisierte Testsuite überprüft dies. Das `auf AsyncLocalStorage basierende` Request-Context-Plugin der Plattform setzt das Prädikat durch; Abfragen außerhalb des Request- Kontexts (geplante Aufgaben, Batch-Jobs) müssen sich explizit davon ausnehmen und den Grund dafür dokumentieren.

Für I2 (Herkunftsauthentizität): Für jeden Datensatz `r` gilt: `recompute_provenance_hash(r.metadata.o` `== r.metadata.origin.provenance_hash`; die Serialisierung in kanonischer Form ist im Hydration-Modus stabil (ein Vorfall vom 22.04.2026 , bei dem 25 Unit-Tests einwandfrei bestanden wurden, während die Hashes von realen Mongoose-Dokumenten von denen zum Zeitpunkt der Speicherung abwichen, brachte diese Anforderung zutage). Die Anwendungsfallvalidierung (§12) stellt die Hash-Stabilität über Hydration-Modi hinweg sicher.

Für I3 (richtlinienkonforme Offenlegung): Bei jeder Cross-Route- oder Cross-WebSocket-Emission wird das Effective-Policy-Gate aufgerufen; ein Datensatz, dessen `share_within-Wert` nicht im anerkannten Vokabular enthalten ist, scheitert mit dem Status CLOSED und dem Grund `share_within_unknown_scope`; dies entspricht dem Grundsatz des Projekts *, ehrlich zu sein, was nicht verifiziert werden kann; keine Berechtigungslage herbeizauber*Ein automatisierter Test erstellt Skelette für Föderations-Peer-Szenarien und überprüft das Verhalten des Gates für jedes einzelne.

Für I4 (Endgültigkeit der kryptografischen Löschung): Für jeden Datensatz, der mit `„delete_must_be_cryptographic"` gekennzeichnet ist, zerstört die Löschung den datensatzspezifischen Verschlüsselungsschlüssel im Tenant-Schlüsselspeicher; nachfolgende Leseversuche geben `„unverifiable"` statt `„valid"` zurück; der ruhende Chiffretext ist durch Neuschlüsselung nicht wiederherstellbar.

Für I5 (Integrität des Föderationsmanifests): Ein Föderationsmanifest enthält Signaturen beider Parteien; `verify_signature(manifest, party_a.did_document) == true && verify_signature(manifest, party_b.did_document) == true`; die Föderation wird nicht aktiviert, wenn eine der beiden Prüfungen fehlschlägt; ein statischer Test stellt sicher, dass kein Codepfad die Föderation ohne diese Prüfungen aktiviert.

Für I6 (Rekonstruierbarkeit der Prüfprotokolle): Für jede mandantengebundene Ereignisfolge kann die Beweiskette für jeden betroffenen Datensatz durch Lesen der signierten Einträge rekonstruiert werden; kein Ereignis bleibt unerwähnt; der Audit-Log-Writer der Architektur wird von einem einzigen Engpasspunkt aus aufgerufen, der nicht durch einen Controller umgangen werden kann, der den Aufruf überspringt.

Für I7 (Ehrlichkeit der souveränen Portabilität): Bei einer Exportanfrage gemäß Artikel 15 enthält die Antwort (a) das kanonische Bundle, (b) die Zurückhaltungsliste, in der jeder ausgeschlossene Datensatz und der grund dafür aufgeführt sind, (c) eine signierte Quittung, die beides abdeckt. Ein Integrationstest stellt sicher, dass zurückgehaltene Datensätze ausgeschlossen *und* aufgelistet werden.

Für I8 (Off-Platform-Mining-Grenze): Die Laufzeit- Inferenzschicht wird auf einer vom Mandanten kontrollierten oder von der Community als vertrauenswürdig eingestuften Infrastruktur gehostet (im Falle der Plattform auf der EU-souveränen OVH France oder die neuseeländische Catalyst Cloud

oder ein ausgewiesenes Home-eGPU-Failover). Es gibt keine Anfrage an einen von den USA kontrollierten Inferenz-Endpunkt im Produktions- Anfragepfad. Eine durch Code-Review durchgesetzte Anbieter-Verbotsregel listet zulässige und verbotene Anbieter explizit auf.

Für I9 (keine biometrische Datenerfassung): Ein Code-Grep gegen den Quellcode-Baum der Plattform liefert keine Treffer für Namen von Bibliotheken oder APIs zur biometrischen Datenverarbeitung; eine Laufzeitprüfung der Datenspeicher der Plattform liefert keine Felder mit biometrischem Format; ein statischer Test stellt sicher, dass nirgendwo im Quellcode der Plattform eine Bibliothek zur biometrischen Datenverarbeitung importiert wird. Die architektonische Verpflichtung ist in der Anbieter-Verbotsregel (§13.1) festgeschrieben und wird bei jeder Änderung durch eine Codeüberprüfung verifiziert. Die mitgliederseitige, gerätelokale biometrische Entsperrung eines vom Mitglied kontrollierten Zugangsdaten-Tresors – Apple Secure Enclave, Android StrongBox, Hardware-Token-Tresore – ist zulässig und für die Plattform architektonisch unsichtbar; die biometrischen Daten überschreiten niemals die Plattformgrenze.

Das Bedrohungsmodell ist nicht erschöpfend. Es ist das Modell, gegen das die Architektur *bekanntermaßen* Schutz bietet, mit benannten Prädikaten, die der Betreiber und externe Prüfer testen können. Nicht oben aufgeführte Bedrohungen (Denial-of-Encryption-Angriffe, Seitenkanalangriffe gegen den Schlüsselspeicher, Supply-Chain-Angriffe gegen das Framework Tractatus) liegen außerhalb des Geltungsbereichs dieses Papiers, werden jedoch im Rahmen der Betriebsdisziplin des Projekts verfolgt.

---

5. Entwurfsprinzipien

5.1 Mandantenisolierung als Grundlage, nicht als Feature

Das oberste Gebot der Architektur ist, dass die Mandantenisolierung die grundlegende Primitive ist. Jede Datenbankabfrage wird nach `tenantId` gefiltert. Der Filter wird durch ein Datenbank-Plugin durchgesetzt, das in einem `AsyncLocalStorage-Anforderungskontext` ausgeführt wird; Abfragen außerhalb des Anforderungskontexts (geplante Aufgaben, Batch-Jobs) müssen sich explizit abmelden und den Grund dafür dokumentieren. Es gibt keine Plattform-Administratorrolle mit mandantenübergreifendem Zugriff auf Inhalte; ein Plattform-Administrator kann Mandanten erstellen und verwalten (Infrastrukturbetrieb), aber keine Mandanteninhalte lesen. Dies ist keine Konfigurationsoption – es wird im Code durchgesetzt, und jeder Versuch eines mandantenübergreifenden Zugriffs wird als Sicherheitsmangel behandelt.

Die Vorgehensweise ist dauerhaft. Ein einzelner interner Speichereintrag mit der Kennzeichnung „never truncate“ (niemals kürzen) formuliert das Prinzip: *„Mandantenisolierung IST das Produkt. Ohne sie gibt es keine*

Souveränität.“ Dies ist eine interne Entwicklungsregel, die durch Code-Reviews und automatisierte Tests durchgesetzt wird, die fehlschlagen, wenn eine Abfrage ohne Mandantenfilter erstellt wird.

5.2 Metadaten für souveräne Datensätze als einheitliches Schema

Jedes Inhaltsmodell, das Teil der Souveränitätsgeschichte ist, enthält denselben Metadatenblock, der über ein Datenbank-Plugin angewendet wird:

```
metadata: {
  origin: {
    author_did, kaitiaki_did, collective_id,
    tikanga_under_which_shared, created_at,
    provenance_hash, provenance_algorithm
  },
  policy: {
    share_within, share_exclude_jurisdictions, share_include_jurisdictions,
    collective_consent_required, collective_consent_body,
    train_flag, conflict_resolution_directive,
    delete_must_be_cryptographic, delete_propagates,
    expiry, individual_overrides_respected
  },
  Verschlüsselung: { Schlüssel-ID, Algorithmus },
  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 }
}
```

Das Schema ist identisch für alle mandanten-generierten Inhaltsmodelle — Story, Poll, Event, Media, Album, Comment, ChatMessage, Deliberation, Correspondence, NewsPost, Resource, CommunityResource, ResourceBooking — sowie für eine erweiterte Reihe eingebetteter Oberflächen (Unterdokument-Abdeckung von EventMenu, Edition und ähnlichen). Der Erstellungs-Pfad jedes Modells leitet den Ursprung über einen gemeinsamen Helper ab; der Pre-Save-Hook des Plugins berechnet den Provenienz-Hash und signiert den Erstellungs-Eintrag; der Post-Save-Hook speichert den Verifizierungsstatus im Cache; Lesevorgänge versehen jeden Datensatz mit einem Verifizierungsfeld, das den Verbrauchern die Aktualität des Caches anzeigt. Die Einheitlichkeit ist der Kernpunkt: Es gibt keine modellspezifische, maßgeschneiderte Souveränitätsimplementierung und somit kein modellspezifisches Risiko einer Souveränitätsregression.

5.3 Kryptografische Provenienz mit Algorithmusflexibilität

Die Provenienz wird als SHA-256 über eine kanonische JSON-Serialisierung der erforderlichen und optionalen Felder des Ursprungs berechnet. Der Algorithmus wird in `provenance_algorithm` benannt, sodass eine zukünftige Migration zu einer anderen kryptografischen Primitive (z. B. NIST-Post-Quantum-Kandidaten) keine Schemaänderung erfordert – lediglich einen neuen Eintragspunkt in derselben kanonischen Form. Signaturvorgänge auf Proof-Chain-Einträgen enthalten ebenfalls ihr `Algorithmusfeld`; der Krypto-Agilitäts-Wrapper der Plattform unterstützt derzeit Ed25519 und ist so strukturiert, dass er zusätzliche Algorithmen ohne Änderungen an den Aufrufstellen akzeptiert.

Dies ist beabsichtigt. Langlebige Datensätze überdauern die kryptografischen Primitive, mit denen sie signiert wurden. Eine Architektur, die ihre Primitive fest codiert, kann keinen Souveränitätsanspruch erfüllen, der länger andauert als die Lebensdauer der Primitive. 5.4

5.4 Richtlinienvererbung mit Berechnung der effektiven Richtlinie an der Lese- Grenze

Eine Richtlinie ist kein einzelnes Feld, sondern eine Hierarchie. Jeder Mandant verfügt über eine souveräne Konstitution, die seine Standardwerte festlegt; jede Untergruppe kann diese überschreiben; `der metadata.policy-Block` jedes Datensatzes kann weitere Spezifikationen enthalten. Zum Zeitpunkt des Lesens wird für das anfragende Mitglied eine effektive Richtlinie anhand des Richtlinienstapels des Datensatzes berechnet. Die Policy Inheritance Engine führt diese Berechnung durch; die Kontrolle wird an der Routengrenze durch Aufrufe pro Liste und pro Detail durchgesetzt.

Die Engine wird auf mehreren Ebenen getestet: Unit-Tests pro Regel, Use-Case-Validierung anhand von aktiven lokalen Datenbanken und eine Disziplin, die sicherstellt, dass Tests zwar in Mocks funktionieren, Use-Cases jedoch beweisen, dass sie in der Realität funktionieren. Diese letzte Verpflichtung – verinnerlicht nach einem Vorfall, bei dem eine umfangreiche Unit-Test-Suite für eine Funktion, die in der Produktion nicht verkabelt war, einwandfrei bestand – ist in der Betriebsdisziplin des Projekts dokumentiert.

Drei Filteroptionen schränken den Zugang auf bestimmte Zugriffsmuster ein: „origin-only“ beschränkt Lesezugriffe auf die Autoren-Identifikatoren des Datensatzes; „group-scope“ beschränkt Lesezugriffe auf Mitglieder der `„collective_id"-Untergruppe` des Datensatzes; der strenge Modus von „unknown-scope“ schlägt CLOSED bei jedem `share_within-Wert`, den das Gate nicht erkennt – eine mehrschichtige Verteidigung gegen falsch konfigurierte Mandantenkonfigurationen oder aus der Föderation importierte Datensätze, die Bereichswerte außerhalb des von der Plattform anerkannten Satzes enthalten.

5.5 Bilaterale Föderation in der Produktion

Föderation im Sinne dieses Papiers ist die enge technische Vereinbarung gemäß §2.4 und §4. Die Konstitutionen zweier Mandanten stimmen hinsichtlich des begrenzten Zwecks der Föderation überein; beide Betreiber unterzeichnen das Föderationsmanifest; der Datenfluss erfolgt direkt zwischen den beiden Mandanten; jeder kann jederzeit widerrufen. Das Föderationsmanifest selbst ist ein souveräner Datensatz – es enthält seine eigene Herkunft, seine eigene Richtlinie, seine eigene Nachweiskette und seinen eigenen Verifizierungs-Cache.

Die Föderationsinfrastruktur wird End-to-End in der Plattform bereitgestellt: das Vereinbarungsmodell, der Vereinbarungsdienst, die Routenoberfläche, eine Administrator-Benutzeroberfläche, ein Audit-Log-Pfad und eine umfassende Negativtest- Matrix, die bereichsgebundene Lesevorgänge, das Blockieren von mieterübergreifenden Schreibvorgängen, die Vollständigkeit des Audit-Logs, die Zitierdisziplin, Caching/Veralterung, Datenzustände in Randfällen, Autorisierungsgrenzen und Namensraumkonflikte abdeckt. Live-Föderationsverbindungen zwischen unabhängigen Mandanten stehen nach der ersten Multi-Instanz-Bereitstellung an; das bilaterale Muster ist aufgebaut, die Bereitstellungen jedoch noch nicht. §7 berichtet ausführlich über die Implementierung.

5.6 Mitgliedergeführte souveräne Portabilität

Ein Mitglied, das seinen Mandanten verlassen möchte – um zu einem anderen Mandanten zu wechseln, der nach demselben Architekturmodell arbeitet, um seine Daten in eine andere Community zu übertragen oder um das Recht auf Auskunft gemäß Artikel 15 der DSGVO zu erfüllen –, kann dies über einen kanonischen Export tun. Der Export enthält jeden Datensatz, in dem das Mitglied als Autor, Kaitiaki oder anderweitig als betroffene Person genannt ist; jeder Datensatz überträgt seine Beweiskette mit; die empfangende Partei kann die Kette anhand des veröffentlichten DID-Dokuments des Quell-Tenants überprüfen, ohne einem der Betreiber vertrauen zu müssen. Datensätze, deren Richtlinie den Export verbietet (z. B. eine unter Bedingungen der kollektiven Zustimmung eingereichte Beratung), werden im Exportmanifest als zurückgehalten aufgeführt, wobei der Grund der Richtlinie angegeben wird.

Dies ist der architektonische Rahmen von Artikel 15 der DSGVO: kein zweckgebundener Zugriffsendpunkt, sondern dieselbe Exportpipeline, die die Architektur für alle Bewegungen souveräner Datensätze nutzt, instanziiert für den Fall „betroffene Person als Mitglied“. §8 beschreibt die Implementierung, einschließlich des Erfassungspfads des empfangenden Mandanten, der den Migrationskreislauf schließt.

---

6. Architektonische Implementierung

Dieser Abschnitt beschreibt die Komponenten, die die in §5 dargelegten Entwurfsprinzipien in Code umsetzen. Jede davon ist an beiden Infrastrukturstandorten in Betrieb (EU-hohe OVH France; neuseeländisch-hohe Catalyst Cloud) und anhand des Quellcodes sowie der laufenden API-Oberfläche überprüfbar. Entsprechend der IP-Perimeter-Strategie (§13) beschreibt dieser Bericht architektonische Komponenten und deren Interaktionen und nicht die Quellpfade einzelner Dateien.

6.1 Kryptografische Provenienz-Primitive

Die Provenienz-Primitive berechnet SHA-256 über eine kanonische JSON-Serialisierung der erforderlichen und optionalen Felder der Quelle. Der Einstiegspunkt erzeugt den Hash; ein Verifizierer berechnet diesen neu und vergleicht ihn mit dem gespeicherten Hash. Die Algorithmus-Kennung wird mit dem Datensatz übertragen. Ein Hilfsmittel für die kanonische Form eliminiert die vom Hydration-Modus abhängige Enumeration – ein Fehlermodus, der bei der Validierung von Anwendungsfällen zutage trat, bei der ein Serialisierer, der die enumerierbaren Eigenschaften eines ORM-Unterdokuments durchlief, Hashes erzeugte, die je nach Hydration-Modus voneinander abwichen, während eine umfangreiche Unit-Test-Suite für Payloads aus einfachen Objekten einwandfrei bestand. Die Behebung erfolgte durch einen einzigen Normalisierungsschritt; die Vorgehensweise, die dies aufdeckte (Validierung von Anwendungsfällen anhand von Live-Datenbanken, nicht nur anhand von Mock-Tests), ist nun Teil der Betriebsnormen des Projekts.

6.2 Signierung der Proof-Chain bei Erstellungen, Aktualisierungen und Löschungen

Jeder Schreibvorgang in einen mit einem Sovereign-Tag versehenen Datensatz fügt einen signierten Eintrag an die Proof-Chain des Datensatzes an. CREATE-Einträge werden mit dem Proof-Signing-Schlüssel des Mandanten (bereitgestellt über den Mandantenschlüsselspeicher, §6.6) signiert und binden den Eintrag an den Provenance-Hash des Datensatzes. UPDATE-Einträge bei Schreibvorgängen im Dokumentmodus werden nur ausgegeben, wenn sich souveränitätsrelevante Pfade geändert haben (ausgenommen Buchhaltungsfelder wie `updatedAt`); die Liste der geänderten Pfade wird erfasst. UPDATE-Einträge im Abfragemodus folgen dem gleichen Schema, berechnet aus der Differenz zwischen Vor- und Nachbild- Dokumenten bei `updateOne`, `updateMany`, `findOneAndUpdate` und zugehörigen Pfaden. DELETE-Übergänge werden von zwei Hook-Ebenen verarbeitet – einem Hook im Dokumentmodus und einem Hook im Abfragemodus, die Einzel-, Batch- und findAndDelete-Varianten abdecken. Beide Ebenen erzeugen einen Tombstone-Datensatz, der den signierten Lösch-Eintrag als Nachweis für die Löschung enthält; Tombstones im Abfragemodus sind über das Feld `policy_evaluated_by` deutlich von Tombstones im Dokumentmodus zu

unterscheiden. Eine separate Komponente erweitert dies auf das Governance-Queue-Modell und stellt sicher, dass auch governance-interne Löschungen eine signierte kryptografische Spur hinterlassen.

6.3 Verifizierung, Caching und Integration in den Lesepfad

Die Verifizierung der Beweiskette erfolgt bei der Erfassung und wird im Verification-Cache-Block des Datensatzes zwischengespeichert: der Zeitpunkt der letzten Verifizierung, der SHA-256-Hash der kanonisierten Beweiskette zu diesem Zeitpunkt, die verifizierten Algorithmen und die nächste Frist für die erneute Verifizierung (standardmäßig 90 Tage; vom Mandanten über die Konstitution konfigurierbar). Der Verifizierer stellt drei Einstiegspunkte bereit: eine Verifizierung und Zwischenspeicherung bei der Erfassung, eine synchrone Cache-Prüfung beim Lesen und einen geplanten Batch-Durchlauf.

Die Verkabelung ist einheitlich. Ein Pre-Save-Hook berechnet die Provenienz und signiert den Erstellungs-Eintrag. Ein Post-Save-Hook löst nach jedem Schreibvorgang „Verify-and-Cache“ aus, entprellt durch einen In-Flight-Schlüssel, um Storm-Bedingungen zu verhindern. Eine geplante Aufgabe wird täglich für die vom Mandanten generierten Inhaltsmodelle ausgeführt und verarbeitet abgelaufene Cache-Einträge in Batches. Der Post-Save-Hook wird bei Erstellungen und bei für die Souveränität relevanten Aktualisierungen ausgelöst; ein Pfadlistenfilter schließt Buchhaltungspfade aus, damit die eigenen Schreibvorgänge des Verifizierers den Hook nicht in eine Endlosschleife versetzen; reine Buchhaltungs-Speicherungen überspringen den Verifizierer und beschränken den Aufwand für die erneute Verifizierung auf echte Änderungen der Souveränität .

Der Lesepfad vervollständigt die Oberfläche. Jede API-GET-Antwort auf einen mit einem Souveränitäts-Tag versehenen Datensatz enthält ein Verifizierungsfeld: kompakt `{valid, reason}` bei Listenantworten, ausführliche Zusatzangaben (verified-at, re-verify-after, algorithms-verified) bei Detailantworten. Die Implementierung ist einheitlich: Ein einziger Decorator-Helper wird von den Lean- und Aggregate-Pfaden jeder Route aufgerufen.

6.4 Policy-Vererbungs-Engine und Durchsetzung auf Gruppenebene

Die Policy Inheritance Engine liest aus der Mandantenkonstitution, den Untergruppenmitgliedschaften des anfragenden Mitglieds, dem Policy-Block des Datensatzes und der angeforderten Operation (lesen/schreiben/exportieren/löschen). Sie gibt eine wirksame Richtlinie mit expliziten Verstoßgründen zurück, wenn eine Anfrage fehlschlägt. Drei Filteroptionen schränken den Zugriff gemäß §5.4 ein.

Die Durchsetzung auf Gruppenebene hängt davon ab, dass Datensätze eine gültige `collective_id` enthalten. Ein Helper validiert eine vom Aufrufer bereitgestellte Untergruppen-ID anhand von drei Einschränkungen (Format, Mandantenbereich, Zugriffsberechtigung) und gibt einen atomaren Kontext

zurück – atomar, da `collective_id` ohne `share_within: ['group']` rein dekorativ ist (die Überprüfung würde nicht durchgesetzt werden). Acht Pfade zur Inhaltserstellung (Poll, Event, Story, Album, Deliberation, ChatMessage, Carpool, Resource) akzeptieren die Untergruppen-ID aus dem Request-Body und leiten sie über den Helper weiter. Die Abwärtskompatibilität bleibt erhalten: Aufrufer, die das Feld weglassen, erstellen wie bisher Datensätze im Tenant-Bereich. Formular-basierte UI-Auswahlfelder bieten die Auswahl von Untergruppen auf der Ebene des Erstellungsformulars über alle acht Oberflächen hinweg an.

Der Strict-Modus für unbekannten Geltungsbereich schließt eine in früheren Iterationen vorhandene Fail-Open-Lücke. Ein plattformweiter Satz anerkannter Geltungsbereichswerte definiert das Vokabular; jeder Wert außerhalb dieses Satzes wird nun mit einer benannten Begründung abgelehnt, es sei denn, ein anerkannter Geltungsbereich im selben Satz gewährt bereits Zugriff. Dies ist die grundsätzliche Haltung des Projekts – *ehrlich zu sein, was nicht überprüft werden kann; keine Berechtigung dafür zu erfinden* – angewandt auf das Read-Path-Gate.

6.5 Editor für die souveräne Verfassung

Die souveräne Verfassung eines Mandanten kann vom Mandantenadministrator über einen dedizierten Pfad und ein Frontend bearbeitet werden. Der Editor zeigt die verfassungsmäßigen Standardeinstellungen (Standard-Auflösungsmodus, Standard-Exportmodus, Standard-vermutete Berechtigung, Verschlüsselungsmodell), eine Kategorietabelle, die die kanonischen Inhaltsmodelle festlegt und mandantendefinierte benutzerdefinierte Kategorien zulässt, sowie mehrsprachige Unterstützung für Englisch, Deutsch, Französisch, Niederländisch und Te Reo Māori an. Die Übersetzungen ins Te Reo Māori wurden mithilfe des Übersetzungstools des Projekts (DeepL, das Te Reo Māori unter dem Sprachcode `MI` unterstützt – eine Tatsache, die von externen Kommentatoren regelmäßig falsch angenommen und innerhalb des Projekts selbst korrigiert wurde) erstellt und stichprobenartig auf Sinnhaftigkeit überprüft.

Ein verfassungsrechtliches Übergangsfenster bedeutet, dass Mandanten, die ihre Verfassung bearbeiten, einen Hinweis sehen, der darauf hinweist, dass die Änderung erst nach dem Übergang verbindlich wird; dies ist die verfassungsrechtliche Vorbedingung, die einen Verfassungsentwurf von einer verbindlichen Verfassung unterscheidet. Ein separates Gate (das „Sovereign-Constitution-Gate“) erzwingt strikt den 403-Fehler für Mandanten, die nach dem Cutover-Datum erstellt wurden und denen erforderliche Sovereign-Abschnitte fehlen, mit integrierter Immunität gegen die Sperrung für bestimmte Mandanten der Plattform-Infrastruktur. 6.6 Mandanten-Schlüsselspeicher

6.6 Schlüsselspeicher des Mandanten

Die Verschlüsselungs- und Signaturschlüssel jedes Mandanten befinden sich in einem mandantenbezogenen Schlüsselspeicher mit Funktionen zur Generierung, Abfrage, Rotation und Vernichtung. Schlüssel werden durch Identifikatoren adressiert, die im Verschlüsselungsblock jedes Datensatzes gespeichert sind. Die kryptografische Löschung eines Datensatzes – durch das Flag `„delete_must_be_cryptographic"` geregelt – erfolgt durch die Vernichtung des datensatzspezifischen Verschlüsselungsschlüssels im Mandantenschlüsselspeicher, wodurch der Chiffretext des Datensatzes aus dem persistenten Zustand nicht mehr wiederherstellbar ist.

6.7 Dezentrale Veröffentlichung von Identifikatoren

Dezentrale Identifikatoren von Mandanten und Mitgliedern folgen der W3C-DID- Spezifikation [11] und werden unter der Domäne des Mandanten veröffentlicht (`/.well-known/did.json` für das Mandanten-DID-Dokument; `/.well-known/did/members/${slug}/did.json` optional für Mitglieder-DIDs). DID-Dokumente enthalten die Verifizierungsmethoden des Mandanten, die zum Signieren von Proof-Chain-Einträgen verwendet werden; ein externer Verifizierer, der das DID-Dokument des Mandanten besitzt, kann jeden signierten Eintrag eines Datensatzes verifizieren, einschließlich Einträgen in Datensätzen, die gemäß §8 an einen anderen Mandanten exportiert wurden.

6.8 Governance-Warteschlange

Das Governance-Queue-Modell erfasst Fälle, die eine Entscheidung durch den Mandanten-Arbiter erfordern: Richtlinienverstöße, Anträge auf Konfliktlösung, von Mitgliedern initiierte Löschanträge, die einer Governance-Genehmigung bedürfen. Lebenszyklusstatus – erstellt → in Prüfung → entschieden → umgesetzt (oder abgelehnt) – sind überübergangsgesteuert; jede Entscheidung und jede Umsetzung hinterlässt signierte Trace-Einträge, die der Mandant aus seiner eigenen Datenbank rekonstruieren kann. Die Durchsetzung von Fristen erfolgt automatisch gemäß der verfassungsmäßigen Standardauflösung des Mandanten, wenn ein Eintrag seine Nachfrist überschreitet.

6.9 Export-Wrapper mit Sichtbarkeitsüberlagerung für Nicht-Administratoren und symmetrischer Protokollierung

Jeder Export souveräner Datensätze durchläuft einen Wrapper, der drei Bedingungen prüft: Jeder Datensatz enthält eine Herkunftsangabe; jeder Datensatz gehört dem anfragenden Mandanten; der Vollmodus erfordert die Rolle „Mandantenadministrator“. Die Modi „Hash“ und „Aggregate“ stehen nun auch normalen Mitgliedern über ein Sichtbarkeits-Overlay zur Verfügung, das Datensätze auf den Lesehorizont des Aufrufers filtert, bevor die Projektion erstellt wird – Umgehung des Eigentümers; Regeln pro Sichtbarkeitsstufe; Fail-Safe bei Fehlern beim Vorladen von Untergruppen. Verstöße führen zu einem

Eintrag im Governance-Audit-Log mit einer Begründung. Erfolgreiche Exporte schreiben ebenfalls einen Audit-Eintrag mit Metadaten zum Erfassungsmodus (vollständig/Hash/aggregiert), der Datensatzanzahl vor und nach der Filterung, der Aufschlüsselung nach Modellen und der Identität des Aufrufers. Jeder Export – ob erfolgreich oder mit Verstößen – ist aus dem Audit-Protokoll rekonstruierbar; kein Export erfolgt im Hintergrund.

6.10 Einheitliche Migration von Sovereign-Records über die vom Mandanten generierten Inhaltsmodelle

Der Metadatenblock für souveräne Datensätze wird einheitlich über die mietergenerierten Inhaltsmodelle angewendet. Die Migration erfolgte nach Möglichkeit verzögert (Datensätze erhalten die Metadaten beim ersten Schreiben unter dem neuen Schema) und bei Bedarf sofort (ein einmaliges Skript füllte die Provenienz für den bestehenden Datensatzbestand). Derselbe Metadatenblock erstreckt sich auf eingebettete Unterdokument-Oberflächen (EventMenu, Edition und ähnliche) unter einer einheitlichen Plugin-Erweiterung. Der Verifizierungscache wird über den operativen Mandantensatz an beiden Produktionsstandorten gefüllt; der kleine Restbestand an Altdatensätzen ohne Provenienz-Hash wird als `nicht verifizierbar` statt als `gültig` gekennzeichnet – die architektonische Entscheidung lautet, das, was nicht verifiziert werden kann, offenzulegen, anstatt einen Cache dafür zu synthetisieren.

6.11 Worker und WebSocket Richtlinienabgleich

Die asynchrone Worker-Ebene wendet die verfassungsmäßige Richtlinie des Mandanten auf die von ihr erstellten Datensätze an. Die beiden im Geltungsbereich befindlichen Create-Path-Worker (E-Mail-zu-Inhalt-Verarbeitung; Dokumentenscan) rufen einen gemeinsamen Helper auf, der aus den Metadaten des ursprünglichen Auftrags (Mandanten-ID; ID des ursprünglichen Mitglieds; ID der ursprünglichen Untergruppe, falls zutreffend) einen Richtlinienkontext zusammensetzt und`metadata.origin` sowie `metadata.policy` zum Zeitpunkt der Erstellung auf den Datensatz setzt. Worker, die bestehende souveräne Datensätze aktualisieren (OCR-Anreicherung hochgeladener Beiträge; Medienoptimierung; Story- Extraktion; Sprachvalidierung), bewahren die zum Zeitpunkt der Erstellung festgelegte Richtlinie bei und benötigen den Helper nicht. Worker, die keine souveränen Inhalte erzeugen (Orchestrator-Koordination; Warteschlangenscan; Transkriptionspipelines, die operative Warteschlangendatensätze verändern), wurden im Rahmen des Umfangs geprüft und es wurde bestätigt, dass sie den Helper nicht benötigen. Die WebSocket- Oberfläche ist über einen empfängerbezogenen Broadcast-Filter mit derselben Berechnung der effektiven Richtlinie verbunden; bevor eine Chat-Nachricht einen Empfänger-Socket erreicht, wird das Sichtbarkeitsprädikat für diesen Socket ausgewertet, und die Nachricht wird ausgelassen, wenn die Sichtbarkeitsprüfung fehlschlägt. Föderations- Broadcasts werden unverändert weitergeleitet – die Sichtbarkeit in der Föderation wird auf der Ebene des

Föderationsdienstes entschieden, nicht auf der Ebene des Broadcasts.

6.12 Primitive zur Verdichtung der Beweiskette

Eine Primitive zur Verdichtung der Beweiskette ersetzt einen zusammenhängenden Teilbereich der Beweiskette eines Datensatzes durch einen einzelnen signierten Zusammenfassungs-Eintrag, dessen Nutzdaten aus dem SHA-256-Hash des kanonischen JSON der ersetzten Teilkette bestehen. Die Verifizierung eines komprimierten Eintrags erfolgt in zwei Modi: Ein kostengünstiger Standardmodus behandelt den komprimierten Eintrag als einen einzelnen signierten Schritt, der durch den Zusammenfassungs-Hash verankert ist; ein Vollmodus ruft die archivierte Teilkette vor der Komprimierung ab und verifiziert Eintrag für Eintrag. Die Primitive ist je nach Mandantenkonfiguration aktivierbar; standardmäßig ist sie deaktiviert. Die Anwendung auf aktive Mandanten-Beweisketten erfolgt nach dem Zeitplan des Betreibers.

6.13 Nachrüstung von Tombstones

Eine Tombstone-Nachrüstung-Primitive signiert bereits vorhandene Klartext-Tombstones aus der Zeit vor der Einführung der Proof-Chain-Signierung, sodass der Audit- Trail über die gesamte Mandantengeschichte hinweg einheitlich ist. Die Nachrüstung erfolgt pro Mandant, idempotent und wiederaufnehmbar, und fügt einen signierten Eintrag neben den ursprünglichen Klartextfeldern hinzu, ohne diese zu löschen. Die Primitive wird vom Betreiber gesteuert; bisher wurden noch keine Tombstones von Produktionsmandanten nachgerüstet.

6.14 Rahmenwerk Konsultation als Prüfpfad

Jeder architektonischen Entscheidung bei der Entwicklung der Plattform geht eine Framework-Konsultation voraus: ein dokumentierter Entscheidungsprotokoll, in dem die konsultierten Dienste, die bedingungsliste pro Dienst und das Ergebnis aufgeführt sind. Konsultationen werden in lokalen sowie in EU-souveränen und neuseeländisch-souveränen Produktionsdatenbanken aufgezeichnet. Die Aufzeichnung erfolgt automatisiert durch entscheidungsspezifische Skripte; die Dokumentationsform ist eine entscheidungsspezifische Markdown-Datei unter `docs/framework-consultations/`. Die Disziplin der Aufzeichnung – drei Einfügestellen pro Konsultation, damit der Verlust eines einzelnen Hosts die Audit-Position nicht gefährdet – ist der Beitrag; der Wert liegt in der Reproduzierbarkeit und Überprüfbarkeit, nicht in der Anzahl der Datensätze.

Dies ist kein „Virtue Signalling“. Die Konsultation ist der Mechanismus des Projekts, um architektonische Entscheidungen an beobachtbare Artefakte zu binden: Ein zukünftiger Leser kann fragen, *welche Bedingungen die Read-Path-Integration behandelt hat,* und die Antwort findet sich in der Datenbank. Das Arbeitspapier zum Tractatus-Framework [1] dokumentiert das Muster aus der Perspektive des Frameworks; dieser Beitrag dokumentiert eine Instanz davon auf

der Plattformseite, wobei das Konsultations-Ledger Teil der Evaluierungsfläche bildet (§12).

---

7. Bilaterale Föderation in der Produktion

Das bilaterale Föderationsmuster ist durchgängig aufgebaut und verfügt über eine umfangreiche Verifizierungsfläche; Live-Föderationsverbindungen zwischen unabhängigen Mandantenbereitstellungen stehen noch aus. Die Architektur ist bereit für die erste Multi-Instanz-Bereitstellung; die Bereitstellungen sind noch nicht eingerichtet.

7.1 Das Verbund-Manifest

Eine Föderation zwischen zwei souveränen Mandanten wird als Föderationsvereinbarungsdatensatz konkretisiert, der von beiden Mandanten unterzeichnet wird. Die Vereinbarung legt den begrenzten Zweck fest (Mitfahrgelegenheiten, gemeinsame Veranstaltungsankündigungen, gemeinsame Beratungen, gemeinsame Verwaltung von Kaupapa, domänenübergreifende Lehrplanverweise), die Form des Datenflusses (welche Felder in welche Richtung fließen, welche Transformationen stattfinden, welche Aufbewahrungsfristen auf jeder Seite gelten), die tenantübergreifende Richtlinienauflösung (welche Verfassung regelt Datensätze, die im Rahmen der Föderation erstellt wurden; wie Richtlinienkonflikte gelöst werden), das Widerrufsverfahren (jede Partei kann einseitig widerrufen; der Widerruf ist ein signierter Datensatz; die Weitergabe erfolgt sofort) und die Aufbewahrung von Prüfprotokollen (jeder Mandant bewahrt eine signierte Kopie jeder tenantübergreifenden Interaktion auf).

Das Manifest ist selbst ein souveräner Datensatz. Eine Föderation kann nicht aktiviert werden ohne verifizierte Signaturen beider Parteien unter ihren jeweiligen DID-Dokumenten. Anhang C beschreibt die Schemaform auf Architekturkomponentenebene; spezifische Details zu den Feldsätzen der Implementierung werden gemäß der IP-Perimeter-Richtlinie (§13) zurückgehalten.

7.2 Administrator-Benutzeroberfläche und Audit-Protokoll Ein

Ein Mandantenadministrator verwaltet Föderationsvereinbarungen über eine dedizierte Administrator-Benutzeroberfläche, die den Lebenszyklus der Föderation (vorgeschlagen → akzeptiert → aktiv → widerrufen) darstellt und das Audit-Protokoll anzeigt. Jedes grenzüberschreitende Ereignis – ein Verbundvorschlag, eine Annahme, eine über den Verbund weitergeleitete Abfrage, ein Widerruf – hinterlässt einen signierten Eintrag im Verbund-Auditprotokoll. Das Auditprotokoll ist auf beiden Seiten unabhängig rekonstruierbar; kein Mandant ist für seine eigene Auditposition auf die Aufzeichnungen des anderen angewiesen.

7.3 Negativtestmatrix

Eine Negativtestmatrix (unter Continuous-Integration-Abdeckung) überprüft die Invarianten der Verbundoberfläche. Zwölf Kategorien sind aufgebaut: bereichsgebundene Lesezugriffe (einschließlich einer statischen Garantie, dass keine verbotene Sammlungsreferenz im Code des Verbunddienstes erscheint), mandantenübergreifende Schreibsperren, Vollständigkeit des Audit-Protokolls, Zitierdisziplin, Caching-/Veraltungsverhalten, Datenzustände in Randfällen (fehlende Felder; Unterscheidung zwischen „null“ und „fehlt“), Durchsetzung von Autorisierungsgrenzen und Konfliktlösung im Phase-3-Namespace. Ein Teil der Matrix wird von einem Live-Multi-Tenant-Validator durchlaufen, der den vollständigen HTTP-Stack gegen eine laufende Bereitstellung testet; der Rest wird gegen eine Service-Level-Fixture oder als statische Code-Grep-Assertions ausgeführt.

Der belastendste Test in der Matrix ist eine statische Assertion: Die Federation-Service-Datei wird als Text gelesen, Kommentare werden entfernt, und verbotene Sammlungsnamen werden mit dem ausführbaren Code abgeglichen. Die Assertion ist als CI-Test kodiert, nicht als einmalige Pre-Commit-Prüfung; jede zukünftige Erweiterung der Lesefläche der Federation, die eine verbotene Sammlungsreferenz einführt, führt zum Fehlschlagen der Assertion zum Zeitpunkt der CI.

7.4 Status der Live-Bereitstellung

Live-Föderationsverbindungen zwischen unabhängigen Mandanten stehen noch aus, bis die erste Multi-Instanz-Bereitstellung erfolgt ist. Die Carpool-Föderation – eine Art von Föderation, die eine Reihe von Communities für die reine Koha-Mitfahrvermittlung verbindet – ist das ursprüngliche Ziel der Multi-Instanz-Bereitstellung. Ein Carpool-Mandant befindet sich im Aufbau auf einer neuseeländischen Infrastruktur (Catalyst Cloud); die Multi-Instanz-Föderation wird aktiviert, sobald mindestens zwei Carpool-Mandanten in Betrieb sind. **Gemeinschaften oder Organisationen, die den Multi-Instanz-Einsatz von Mitfahrgelegenheiten als Alternative zu einer souveränen Infrastruktur prüfen – Praktiker im Bereich Gemeinschaftsverkehr, Forscher im Bereich Verkehrsgerechtigkeit, Programme zur ländlichen Resilienz, Nachhaltigkeits- oder Verkehrsgruppen an Universitäten – sind eingeladen, sich bezüglich einer Teilnahme am Pilotprojekt an den korrespondierenden Autor zu wenden.** Iwi-zu-Iwi-Föderations- Implementierungen – bei denen ein Iwi spezifisches Kaupapa-Material mit einem anderen Iwi durch ein unterzeichnetes Manifest teilt und dabei die volle Widerrufskontrolle behält – werden infrastrukturell unterstützt, sind jedoch betreibergeleitet; zum Zeitpunkt dieses Entwurfs wurde noch keine aktive Iwi-zu-Iwi- Föderation aktiviert.

Die in §5.5 dargelegte Formulierung der bilateralen Föderation ist daher eine *architektonische Verpflichtung mit bereitgestellter Infrastruktur und einer*

Verifizierungsoberfläche, nicht ein *eingesetztes Netzwerk aktiver Föderationen*. Die entscheidende architektonische Eigenschaft – dass zwei Gemeinschaften sich zu von ihnen festgelegten Bedingungen auf eine bestimmte, begrenzte Interaktion einigen können, und nur darauf – ist genau das, was die drei Artikel von Te Tiriti für die digitale Infrastruktur implizieren: Die Stammeshoheit über Taonga wird geachtet, da jedes Iwi die volle Autorität innerhalb seines eigenen Tenants behält, und die Föderation untergräbt diese Autorität nicht – sie ermöglicht eine bestimmte, begrenzte Interaktion innerhalb des Rahmens der Architektur.

---

8. Souveräne Portabilität – DSR-Integration

Die sechste Designvorgabe der Architektur (§5.6) lautet, dass ein Mitglied ein Datenbetroffener erster Klasse ist. Ein Mitglied, das seinen Tenant verlassen möchte – um zu einem anderen Tenant unter demselben Architekturmodell zu migrieren, um sein Material in eine andere Gemeinschaft zu übertragen oder um ein Recht des Datenbetroffenen gemäß der DSGVO zu erfüllen – kann dies über einen kanonischen Export tun.

8.1 Das kanonische Export- Bundle

Ein vom Mitglied initiierter kanonischer Export enthält jeden Datensatz, in dem das Mitglied der Autor, der Kaitiaki oder anderweitig als betroffene Person benannt ist. Der Export ist ein paginiertes Bündel über die vom Mandanten generierten, mit Souveränitäts-Tags versehenen Inhaltsmodelle hinweg, einschließlich eingebetteter Oberflächen, wo dies zutrifft. Jeder Datensatz im Bundle enthält seine vollständige Proof-Chain, seinen vollständigen Policy-Block und seinen Provenance-Hash. Das Manifest des Bundles ist selbst vom Quell-Tenant signiert; ein externer Prüfer, der über das DID-Dokument des Quell-Tenants verfügt, kann jeden signierten Eintrag im Bundle überprüfen, ohne einem der beiden Betreiber vertrauen zu müssen. Das Bundle wird je nach Anfrageformat als JSON, CSV oder PDF gerendert; der zugrunde liegende kanonische Inhalt ist in allen Darstellungen identisch.

8.2 Richtlinienkonformer Export und Manifest der Zurückhaltungsliste

Der Export-Wrapper setzt die Richtlinie durch. Datensätze, deren Richtlinie den Export verbietet (z. B. eine unter kollektiven Zustimmungsbedingungen beigesteuerte Beratung; ein Medienobjekt, das einer tikanga-spezifischen Freigabebeschränkung unterliegt), werden im Export-Manifest als zurückgehalten aufgeführt, wobei der Grund der Richtlinie angegeben wird. Das Mitglied erhält sowohl das Bundle als auch die Zurückhaltungsliste; die Zurückhaltungsliste ist selbst signiert, sodass das Mitglied über ein überprüfbares Artefakt verfügt, das belegt, was ausgeschlossen wurde und warum. Die Vorgabe ist die vollständige Offenlegung dessen, was zurückgehalten wird und warum: Ein Versuch, ein

Recht der betroffenen Person als Vorwand für den Zugriff auf Material zu nutzen, auf das das Mitglied keinen legitimen Anspruch hat, stößt auf die Richtlinienbarriere, und die Antwort selbst ist überprüfbar.

Der Mechanismus der Zurückhaltungsliste ist die architektonische Antwort auf einen Konflikt, den Regulierungsbehörden seit Jahren erkennen: Das Auskunftsrecht in Artikel 15 wird durch die Rechte anderer identifizierbarer Personen (Artikel 15 Absatz 4) und durch andere Gründe für eine rechtmäßige Verarbeitung eingeschränkt. Eine Standardimplementierung kann entweder alles zurückgeben (und damit die Rechte anderer Parteien verletzen) oder weniger als angefordert zurückgeben (ohne die Grundlage für den Ausschluss zu erläutern). Die Architektur sieht vor, dass jeder ausgeschlossene Datensatz benannt wird, der grundsätzliche Grund dafür angeführt wird und die Verbindung zwischen beiden Elementen überprüfbar ist.

8.3 Datenaufnahme durch den empfangenden Mandanten (mandantenübergreifende Migration)

Ein Mitglied kann sein kanonisches Exportpaket zu einem anderen Mandanten übertragen, der unter demselben Architekturmodell betrieben wird. Der Importpfad des empfangenden Mandanten überprüft die Beweiskette jedes Datensatzes anhand des DID-Dokuments des Quellmandanten, akzeptiert die Datensätze (sofern die Satzung des empfangenden Mandanten dies zulässt) und setzt die Beweiskette fort – der empfangende Mandant signiert einen `„ingest_via_migration"-Eintrag` für jeden Datensatz und nennt dabei den Quellmandanten sowie den Hash des Bundle-Manifests. Die Identität des Mitglieds wird durch dessen mandantenübergreifende DID festgestellt; die Migration wird auf beiden Seiten als normales Sovereign-Record-Ereignis aufgezeichnet. Eine konstitutionelle Akzeptanzprüfung durch den empfangenden Mandanten ist integraler Bestandteil und nicht optional: Datensätze, deren Richtlinie des Quellmandanten mit den Standardeinstellungen des empfangenden Mandanten unvereinbar ist (z. B. strengere Datenschutzhaltung, die eine freizügigere Absenderrichtlinie ablehnt), werden als ABGELEHNT mit dem entsprechenden Grund aufgeführt. Die Empfangsbestätigung des migrierten Bundles wird vom empfangenden Mandanten signiert und an das Mitglied zurückgesendet, wodurch ein überprüfbarer Abschluss der Migration gewährleistet wird.

Die aktuelle Implementierung des Erfassungspfads des empfangenden Mandanten umfasst die Phasen A–F: Auflösung der Quell-DID, Bündelüberprüfung, Konformitätsprüfung, Erfassung mit Weiterleitung der Proof-Chain, Empfangsbestätigungssignatur und durchgängige, vom Framework konsultierte Integrationstestszenarien. Die Identitätsabgleichung in der v1-Implementierung ist so konfiguriert, dass sie das automatische Onboarding standardmäßig ablehnt – ein migrierendes Mitglied muss bereits Mitglied des empfangenden Mandanten sein, oder der Administrator des empfangenden Mandanten muss die Erstellung der Mitgliedschaft manuell genehmigen, bevor das Bundle eingelesen wird. Dies

ist eine bewusste konservative Entscheidung: Das automatische Onboarding über mandantenübergreifende DIDs weist eine Sicherheitsfläche auf, die eine eigene Designüberprüfung rechtfertigt, und die v1- Implementierung verschiebt dies.

8.4 DSGVO-Artikel 15, 16, 17, 18, 20, 21

Die DSR-Endpunkt-Oberfläche implementiert alle sechs Rechte der betroffenen Personen gemäß DSGVO über dieselbe Export-Pipeline, mit rechtesspezifischen Verhaltensweisen, wo erforderlich:

- **Artikel 15 (Auskunftsrecht):** der kanonische Export, wie in §8.1–§8.2 beschrieben.
- **Artikel 16 (Recht auf Berichtigung):** Mitglieder können eine Korrektur beantragen; der Antrag unterliegt den Richtlinien; akzeptierte Korrekturen hinterlassen einen signierten Eintrag in der Nachweiskette.
- **Artikel 17 (Recht auf Löschung):** Datensätze, die ausschließlich vom Mitglied verfasst wurden und bei denen keine anderen Rechte betroffen sind, können auf Antrag kryptografisch gelöscht werden – der Verschlüsselungsschlüssel pro Datensatz wird im Schlüsselspeicher des Mandanten vernichtet; der Chiffretext wird unwiederherstellbar; ein signierter Tombstone dokumentiert die Löschung. Datensätze, die andere Parteien betreffen (ein Kommentar zur Geschichte eines anderen Mitglieds; ein Beitrag zu einer Mehr-Autoren-Beratung), folgen der verfassungsmäßigen Standardeinstellung für die Löschung mit kollektiver Zustimmung – die Governance-Warteschlange des Mandanten erhält den Antrag, die betroffenen Parteien werden gemäß dem Verfahren des Mandanten konsultiert, und die daraus resultierende Entscheidung wird mit vollständigem Prüfpfad umgesetzt.
- **Artikel 18 (Recht auf Einschränkung):** Die Einschränkung wird als Richtlinienüberschreibung implementiert, die die Verarbeitung verhindert, solange der Antrag anhängig ist; die Überschreibung ist selbst ein souveräner Datensatz- Ereignis.
- **Artikel 20 (Recht auf Datenübertragbarkeit):** das kanonische Bündel von §8.1, mit dem Erfassungsweg des empfangenden Mandanten gemäß §8.3 als architektonische Vervollständigung.
- **Artikel 21 (Widerspruchsrecht):** Der Widerspruch wird im entsprechenden Datensatz vermerkt und wird über das Richtlinien-Gate als datensatzspezifisches Verarbeitungsveto weitergeleitet.

Das 30-tägige Antwortfenster gemäß Artikel 15 wird durch einen Audit-Log-Timer durchgesetzt; versäumte Antworten lösen eine Warnmeldung in der Governance-Warteschlange des Mandanten aus.

8.5 Die Spannung mit den Ausnahmeregelungen des Artikels 17

Der architektonische Rahmen für die Spannung zwischen dem Recht auf Löschung gemäß Artikel 17 und den Ausnahmen in Artikel 17(3) (Meinungsfreiheit; Rechtsansprüche) bedeutet nicht, dass diese Spannung nicht existiert; die Spannung ist real. Die Architektur legt die Lösung explizit fest, in der Verfassung des Mandanten, mit richtliniengesteuerter Umsetzung und mit vollständigem Prüfpfad. Ein Löschungsantrag eines Mitglieds wird in dem Umfang berücksichtigt, wie es der Verfassungsbeschluss zulässt; wenn die Bedingungen für die kollektive Zustimmung ein Mehrparteienverfahren erfordern, wird der Prozess protokolliert und die daraus resultierende Entscheidung (löschen, redigieren, aufbewahren) unterzeichnet. Ein externer Prüfer, der das Prüfprotokoll liest, kann genau rekonstruieren, welche Ausnahme nach Artikel 17 geltend gemacht wurde, von wem, bei welchem Datensatz und mit welchem Ergebnis.

---

9. Benutzeroberfläche für die Stakeholder-Governance

Die Governance-Benutzeroberfläche macht die verfassungsrechtliche Ausrichtung der Plattform, die Kommunikationsrichtlinien, die Entscheidungshistorie, das Konsultationsprotokoll des Rahmenwerks, die Dialogoberfläche und die Überprüfungsoberfläche für Stakeholder sichtbar. Es handelt sich um eine Stakeholder-orientierte Oberfläche, die bewusst so gestaltet ist, dass sie für Gemeindekämmerer und Gemeindevorsteher lesbar ist und nicht nur für Ingenieure. Die Benutzeroberfläche befindet sich in einer dafür vorgesehenen Subdomain des Operations-Hub-Mandanten und wird nach einem einheitlichen Muster auf jede Mandantensubdomain repliziert. Die Phasen 1 bis 7 sind zum Zeitpunkt der Veröffentlichung dieses Dokuments bereits verfügbar; Phase 6 (partizipativer Dialog) und Phase 7 (produktübergreifende Verallgemeinerung) erweitern die Oberfläche von einer schreibgeschützten Überprüfung hin zu partizipativer Governance.

Zwei Muster der Stakeholder-Einbindung ziehen sich durch die Oberfläche. Das erste ist **die Einladung**: Ein Mandantenadministrator versendet eine signierte Stakeholder-Einladung, in der der Eingeladene, die für ihn freigegebenen Oberflächen und die Gültigkeitsdauer der Einladung genannt werden; der Stakeholder nimmt über eine einmalig gültige URL an; die daraus resultierende Sitzung unterliegt denselben Zugriffsrichtlinien wie eine Mitgliedersitzung, wobei der Lesezugriff auf die eingeladenen Oberflächen beschränkt ist. Das zweite Muster ist **die Anfrage**: Wenn ein Stakeholder ohne vorherige Einladung Zugang beantragt, leitet die Plattform die Anfrage an das in der Verfassung des jeweiligen Tenants definierte Verfahren weiter. Die architektonischen Grundelemente – Ausstellung der Einladung, Akzeptanz-Token, signierter Prüfpfad – sind für alle Tenants einheitlich und werden in den folgenden Unterabschnitten beschrieben; das vom Stakeholder initiierte Antragsverfahren

ist pro Village-Instanz in der Verfassung definiert und wird in diesem Dokument nicht näher erläutert. Von der Plattform bereitgestellte Referenzsatzungen sind im Satzungs-Viewer (§9.1) dokumentiert, sind jedoch nicht normativ.

9.1 Satzungs-Viewer (Phase 1)

Der Verfassungsverzerer rendert die stabil verankerte, für Stakeholder bestimmte Zusammenfassung der drei Hauptquellen (die festen Regeln des Projekts, die niemals gekürzten Speicherelemente und die Layer-1- universellen Plattformprinzipien). Der Renderer folgt dem Markdown-Page-Loader-Muster: keine API-Route, kein dynamisches Abrufen; der Viewer ist eine statische HTML-Datei, die das Markdown über HTTPS lädt und rendert. Dieses Muster ist beabsichtigt: Der Viewer ist das einfachstmögliche Artefakt und kann von jedem Prüfer überprüft werden, der HTML und Markdown lesen kann.

9.2 Viewer für die Kommunikationsverfassung (Phase 2)

Der Comms-Constitution-Viewer folgt demselben Muster und legt das für Betreiber bestimmte Kommunikationsregelwerk offen (Kanalstapel, Kadenz, Ablehnungsregeln, „Nur-Entwürfe-niemals-senden“-Regeln). Die aktuell veröffentlichte Version schließt die vom Betreiber eingegebenen Elemente unter der vom Betreiber delegierten Agentenentscheidung ab; nachfolgende Überarbeitungen warten auf die Zustimmung des Betreibers.

9.3 Viewer für das Entscheidungsprotokoll (Phase 2)

Der Decision-Log-Viewer stellt einen kuratierten Index bedeutender Entscheidungen während der gesamten Entwicklung der Architektur dar (architektonische Primitive, Herstellerposition, Datenschutz- und Inhaltsregeln, Prozessdisziplin, Schulung und KI). Sowohl der Constitution-Viewer als auch der Comms Constitution-Viewer verweisen in ihren „Companions“-Abschnitten auf den Decision-Log-Viewer. Der vollständige, für Stakeholder lesbare Pfad – Constitution → Kommunikationsverfassung → Entscheidungsprotokoll – ist auf jeder Mandanten- Subdomain navigierbar.

9.4 Framework Consultation Viewer (Phase 3)

Der Framework-Konsultations-Viewer stellt das Konsultationsprotokoll über eine für Stakeholder lesbare HTML-Oberfläche dar. Der Viewer präsentiert einen aggregierten Index nach Dokumentreferenz (eine Zeile pro Architekturentscheidung, mit konsultierten Diensten, Bedingungen, Urteilen und Daten) sowie eine Detailansicht pro Entscheidung, die die vollständige Liste der Bedingungen und den Urteilsverlauf pro Dienst anzeigt. Der Viewer ist schreibgeschützt; das zugrunde liegende Ledger wird von den automatisierten Skripten der Plattform zur Konsultationsaufzeichnung geschrieben; die Stakeholder lesen, schreiben jedoch nicht.

9.5 Zugang per Gast-Token für Stakeholder (Phase 4)

Eine stakeholder-spezifische Gast-Sitzung gewährt schreibgeschützten Zugriff auf die Governance-Benutzeroberfläche, ohne dass eine vollständige Registrierung als Mandant-Mitglied erforderlich ist. Ein Plattformadministrator versendet eine Einladung an den Stakeholder; die Einladung ist ein signierter Datensatz, der den Stakeholder, die eingeladenen Oberflächen und die Gültigkeitsdauer der Einladung nennt; der Stakeholder akzeptiert über eine einmalig gültige URL; die daraus resultierende Sitzung unterliegt denselben Sicherheitsrichtlinien wie eine Mitgliedersitzung, jedoch mit einem auf die eingeladenen Oberflächen beschränkten Lesezugriff.

Die architektonische Eigenschaft besteht darin, dass die Überprüfung durch Stakeholder selbst eine Interaktion mit souveränen Datensätzen ist: Jede Einladung, jede Annahme, jeder Lesezugriff wird protokolliert, signiert und lässt sich anhand des Prüfpfads rekonstruieren. Ein Geldgeber oder Richtlinienprüfer, der die Governance-Benutzeroberfläche der Plattform überprüft hat, kann einen überprüfbaren Nachweis darüber erstellen, was er wann und anhand welcher Version des zugrunde liegenden Materials überprüft hat.

9.6 Stakeholder-Prüfungsoberfläche (Phase 5)

Eine abschließende Überprüfungsoberfläche fasst das Material der Governance-Benutzeroberfläche zu einem einzigen navigierbaren Index für die Nutzung durch Stakeholder zusammen: ein einseitiger Eintrag, der jeden Artikel der Verfassung, jeden Eintrag im Entscheidungsprotokoll, jede Regel der Kommunikationsverfassung und die jüngste Rahmenkonsultation auflistet, mit Deep-Links zu jedem einzelnen. Die Oberfläche ist der natürliche Endpunkt einer Einladung aus Phase 4; ein Stakeholder, der die Einladung annimmt, gelangt auf die Überprüfungsoberfläche und kann von dort aus navigieren.

9.7 Partizipativer Dialog (Phase 6)

Die Dialogoberfläche der Phase 6 wandelt die schreibgeschützte Governance-Benutzeroberfläche in eine partizipative um. Stakeholder können Kommentare zu Verfassungsartikeln, Einträgen im Entscheidungsprotokoll und Regeln der Kommunikationsverfassung abgeben; Kommentare sind selbst souveräne Datensätze, auf die dieselben Mechanismen hinsichtlich Herkunft, Richtlinien, Proof-Chain und Verifizierungs-Cache angewendet werden. Die situationsbezogene Sprachschicht der Plattform beantwortet Stakeholder-Anfragen aus dem kuratierten Korpus, das die Governance-Benutzeroberfläche selbst verwaltet, wobei das Korpus als Zitieroberfläche dient. Der Schutz vor Halluzinationen ist mehrschichtig: Eine verschärfte Systemaufforderung lenkt das Sprachmodell bei Anfragen außerhalb des Korpus standardmäßig in Richtung Ablehnung, und ein Filter zur Einhaltung der Zitierdisziplin lehnt Antworten ab, die keine Korpusquelle angeben.

9.8 Produkttypübergreifende Verallgemeinerung (Phase 7)

Phase 7 verallgemeinert die Dialogooberfläche aus Phase 6 über die Produkttypen der Plattform hinweg. Jeder Produkttyp verfügt über eigene Dialogkorpuspfade, Vokabulare und Zitiermuster. Phase 7.A liefert die Generalisierung pro Produkttyp; Phase 7.B erstellt das gemeinsame Dialogkorpus mit universellen Mustern; Phase 7.C verknüpft die Anzeigeoberfläche für genehmigte Kommentare inline über die mdsl-Viewer-Seiten hinweg mit dynamischen Ankern und einer öffentlichen Widget-API; Phase 7.D ist die Föderationsoberfläche für die Dialogeebene, die dieselbe bilaterale Föderationsinfrastruktur nutzt, wie in §7 beschrieben (die Negativtestmatrix wird gemeinsam genutzt, nicht separat; die Föderation von Stakeholder-Kommentaren über Village-Grenzen hinweg ist eine spezifische Anwendung des allgemeinen bilateralen Musters); Phase 7.E erfasst die Kommunikationsverfassungsregel und die Ledger-Zeile, die die Einführung der Oberfläche dokumentiert.

Der kumulative Effekt der Phasen 1–7 ist eine Stakeholder-Governance-Oberfläche, die lesbar, überprüfbar, navigierbar, partizipativ, föderationsfähig und einheitlich auf alle Produkttypen der Plattform anwendbar ist – auf Kosten einer erheblichen Verifizierungsfläche (wobei die bilaterale Föderations-Negativtestmatrix den größten Einzelbeitrag leistet) und des disziplinären Aufwands für die Durchführung der Framework-Konsultationsaufzeichnung bei jeder Architekturerweiterung.

---

10. Praxisbeispiel: domänenübergreifende Namenshoheit zwischen zwei situierten Sprachmodulen

Dieser Abschnitt veranschaulicht das Muster der bilateralen Föderation anhand eines Praxisbeispiels, das der korrespondierende Autor aus seiner laufenden Lehrplanentwicklungsarbeit beigesteuert hat. Das Beispiel betrifft die Lehrplanintegration im Grundschulkontext, doch lässt sich das Architekturmuster auf jedes Paar von Gemeinschaften verallgemeinern, deren Haltungen zur Datenhoheit sich an einem bestimmten Punkt domänenübergreifender Autorität überschneiden. Eine separate Darstellung ist im in §11 erwähnten Carpool-Village-Typ verfügbar: Carpool isoliert die Föderationsprimitive von der breiteren, mitgliederorientierten Oberfläche anderer Village-Typen und stellt den Minimalfall dar, unter dem das Föderationsverhalten des Musters isoliert untersucht werden kann. Das vorliegende Anwendungsbeispiel veranschaulicht die Föderation zwischen zwei Domänen mit unterschiedlichen autoritativen Inhalten; die Carpool-Darstellung veranschaulicht die Föderation zwischen zwei Instanzen desselben Village-Typs.

10.1 Die Konfiguration

Betrachten wir zwei situierte Sprachmodule, die jeweils als eigenständiger Tenant auf der Plattform operieren:

- **Ein Modul** für**botanisches Wissen** zu einer regionalen Flora – zum Beispiel ein Modul „Flora of New South Wales“, das einer botanischen Einrichtung gehört, die für die validierte Taxonomie, wissenschaftliche Namen, Verbreitung, ökologische Anmerkungen und Querverweise zu wissenschaftlichen Quellen verantwortlich ist. Die Eigentümer des Moduls pflegen den Inhalt im Rahmen eines kontinuierlichen Verbesserungsprozesses: Neue Entdeckungen werden validiert und integriert; Korrekturen werden unter unterschriebener Autorität herausgegeben; der Korpus ist die maßgebliche Quelle für botanische Referenzen innerhalb des Geltungsbereichs des Moduls.
- **Ein Modul zur Sprachrevitalisierung** für eine indigene Sprache in derselben Region – zum Beispiel ein Modul zu den Aborigine-Sprachen von New South Wales, das einer von der Gemeinschaft geleiteten Sprachbehörde gehört, die für das validierte Lexikon, die Aussprache, die Etymologie, den kulturellen Kontext und die laufenden Revitalisierungsbemühungen verantwortlich ist. Die Eigentümer des Moduls behalten die Autorität über die Sprache und ihre Verwendung, einschließlich der Art und Weise, wie die Sprache Entitäten in der Natur benennt.

Ein Punkt der domänenübergreifenden Autorität ergibt sich bei der *Benennung von Pflanzen*. Jede Pflanze im botanischen Modul kann – neben ihrem wissenschaftlichen Namen – einen indigenen Namen aus dem Lexikon des Sprachmoduls tragen. Historisch gesehen unterstanden diese indigenen Namen der Kontrolle des botanischen Moduls als bibliografische Anhänge. Eine politische Entscheidung zur Wiederherstellung der sprachlichen Souveränität überträgt die Benennungshoheit vom botanischen Modul auf das Sprachmodul: Von nun an ist der kanonische indigene Name einer Pflanze der, den das Sprachmodul angibt .

10.2 Föderation als architektonische Lösung

Die architektonische Lösung ist eine bilaterale Föderation zwischen den beiden Modulen, mit einem Manifest, das die abgegrenzte Interaktion genau benennt:

- **Begrenzter Zweck:** domänenübergreifende Namensreferenz. Das botanische Modul kann das Sprachmodul nach dem kanonischen indigenen Namen einer Pflanze abfragen, wenn ein wissenschaftlicher Binomialname vorliegt. Das Sprachmodul behält die gesamte Autorität über den Namen; das botanische Modul behält die gesamte Autorität über die wissenschaftliche Taxonomie.
- **Datenfluss:** Eine strukturierte Abfrage vom botanischen Modul an das Sprachmodul nennt den wissenschaftlichen Binomialnamen; die Antwort

ist der kanonische indigene Name (oder `„unbekannt"`, falls das Korpus des Sprachmoduls diese Pflanze noch nicht benannt hat). Der Fluss erfolgt *auf Abruf*; eine Batch-Übertragung ist nicht vorgesehen. Das botanische Modul kann Antworten mit einer vom Mandanten konfigurierbaren Gültigkeitsdauer zwischenspeichern.

- **Richtlinienauflösung:** Die Verfassung des Sprachmoduls regelt die Antwort. Befindet sich der Korpus des Sprachmoduls in Überarbeitung und ist ein Name vorläufig ausstehend, enthält die Antwort diesen Status als Feld `„caveats_added"` im Proof-Chain-Eintrag; das botanische Modul gibt den Status an seine Verbraucher weiter.
- **Widerruf:** Jede Partei kann jederzeit widerrufen. Der Widerruf wird sofort wirksam; das botanische Modul stellt die Abfragen ein; zwischengespeicherte Antworten verfallen entsprechend ihrer Gültigkeitsdauer. Nach dem Widerruf findet kein Datenfluss mehr statt. Audit: Jede Abfrage und jede Antwort hinterlässt einen signierten
- **Prüfung:** Jede Abfrage und jede Antwort hinterlässt einen signierten Proof-Chain-Eintrag auf beiden Seiten. Jede Partei kann den vollständigen Verlauf der Föderation aus ihrer eigenen Datenbank rekonstruieren.

10.3 Die Erfahrung der Studierenden

Ein Schüler, der den Lehrplan durcharbeitet, stellt eine Frage: *„Wie lautet der indigene Name für Eucalyptus camaldulensis?“* Die Lehrplanbereitstellung der Plattform leitet die Anfrage an das botanische Modul weiter (das den wissenschaftlichen Binomialnamen als maßgebliche Quelle enthält), und die Föderation leitet die Unterabfrage zur Namensauflösung an das Sprachmodul weiter. Die Antwort wird *aus einer Kombination situierter Sprachmodule zusammengestellt, nicht aus einem großen Sprachmodell der neuesten Generation.* Der Schüler sieht den Namen, die Quellenangabe des Sprachmoduls und einen Hinweis darauf, dass die Antwort von der Föderation bereitgestellt wurde – nicht weil die Föderation für einen Schüler technisch interessant ist, sondern weil Überprüfbarkeit ein Wert des Lehrplans ist.

Die entscheidende architektonische Eigenschaft besteht darin, dass der Schüler eine kuratierte, maßgebliche Antwort erhält, ohne dass ein LLM in den Prozess eingebunden ist. Halluzinationen sind strukturell ausgeschlossen, da kein Modell die Antwort aus einer Wahrscheinlichkeitsverteilung über Trainingsdaten generiert; die Antwort ist eine föderierte Abfrage gegen einen kuratierten Korpus, der vom Rechteinhaber verwaltet wird. Wenn der Korpus keine Antwort enthält, gibt die Föderation `„unbekannt"` zurück – dem Studierenden wird mitgeteilt, dass das System es nicht weiß, eine strukturell korrekte Antwort, die die selbstbewusste Konfabulation eines State-of-the-Art-Modells nicht bieten kann.

10.4 Die architektonischen Lehren

Aus diesem Beispiel lassen sich drei Lehren für die architektonischen Vorgaben in §5 ableiten:

1. **Die domänenübergreifende Übertragung von Hoheitsrechten ist ein Föderationsvorgang.** Wenn die Zuständigkeit für eine Klasse von Referenzen von einer Gemeinschaft auf eine andere übergeht (Botanik → Sprachmodul zur Pflanzenbenennung; Iwi → Kāhui bei einem gemeinsamen Kaupapa; Pfarrei → Diözese bei einem gemeinsamen Veranstaltungskalender), besteht der architektonische Vorgang darin, ein neues Föderationsmanifest zu unterzeichnen, und nicht darin, Daten zwischen Mandanten zu migrieren. Die Daten verbleiben dort, wo sich der Rechteinhaber befindet; die Föderation teilt dem Verbraucher mit, wo er die Abfrage stellen soll.
2. **Die Vermittlung von Lehrplänen über föderierte, kontextbezogene Module ist eine strukturell eigenständige Bereitstellung, die sich von LLM-kuratierten Antworten unterscheidet.** Der Anwendungsfall der Lehrplanvermittlung ist ein starker empirischer Motivator für die Ausrichtung der Architektur gegen die LLM-vermittelte Inhaltsbereitstellung: Wo der Schüler ein Lernender ist, sollte die Antwort autoritativ sein, nicht probabilistisch.
3. **Das Feld „bounded-purpose“ im Föderationsmanifest ist tragend.** Ein Verbund zur Namensauflösung autorisiert das Botanikmodul nicht, den gesamten Korpus des Sprachmoduls abzufragen; er autorisiert nur die benannte Abfrageform. Der Verbunddienst der Plattform lehnt Abfragen ab, die außerhalb der im Manifest festgelegten Form liegen. Dies ist die architektonische Eigenschaft, die es zwei souveränen Gemeinschaften ermöglicht, sich über eine spezifische, begrenzte Interaktion zu verbünden, ohne die Autorität über sonstiges aufzugeben.

Eine Reihe verwandter Föderationsklassen – zwischen dem Sammlungsmodul eines Museums und dem Kulturgutmodul einer indigenen Gemeinschaft; zwischen dem Planungsmodul eines Regionalrats und dem Modul für Kulturerbestätten eines Hapū; zwischen dem Lehrplanmodul eines Schulbezirks und dem Sprachmodul einer Gemeinschaft – weisen dieselbe Struktur auf. Das Beispiel „Flora Sprachen“ wird als kanonisches Beispiel angeführt, da es sowohl die Dimensionen *der Datensouveränität* als auch *des Transfers epistemischer Autorität* gleichzeitig sichtbar macht.

---

11. Sechs dorfartige Konfigurationen – Beispiele aus einer Vorlagenfamilie

Die Architektur wird durch ein Vorlagenmodell ausgedrückt. Eine Mandantenkonfiguration ist keine einmalige Erstellung; es handelt sich um eine Instanziierung der

Vorlage, bei der die Vorlage die Primitive für Souveränitätsdatensätze, das Verhalten der Richtlinienvererbung, die Föderationssemantik, die Governance-Benutzeroberfläche sowie die Form der Governance-Warteschlange festlegt, während die mandantenspezifische Konfiguration das festlegt, was die Vorlage offen lässt: die Verfassung, die Mitgliederstruktur, die Topologie der Untergruppen, die mehrsprachige Locale, die Kohorte der situierten Sprachschicht sowie die Anbieterpräferenzen innerhalb des Rahmens für Anbieterverbote.

Der operative Wert des Vorlagenmodells besteht darin, dass eine neue Konfiguration vom Typ „Dorf“ eine Konfigurationsaufgabe ist und kein Neuaufbau. Der architektonische Wert besteht darin, dass ein Prüfer, der eine Konfiguration vom Typ „Dorf“ untersucht, *dieselbe Architektur* prüft, auf *der* auch jede andere Konfiguration vom Typ „Dorf“ läuft; die Souveränitätsgarantien sind innerhalb der Familie einheitlich, da die Vorlage einheitlich ist.

Die in diesem Artikel beschriebene Plattform ist selbst die Referenzimplementierung der darin dargestellten Architektur. Die Plattform wurde von einem kleinen Team in Neuseeland unter den Einschränkungen von Lieferantenverboten und Souveränitätsauflagen entwickelt – genau jenen Einschränkungen, gegen die die Architektur Schutz bietet. Die Entwicklung unter diesen Einschränkungen brachte die Fehlermodi zutage, gegen die die Architektur schützt, darunter die Versuchung, unter Kostendruck auf Infrastruktur unter US-amerikanischer Gerichtsbarkeit für Speicher oder Rechenleistung zurückzugreifen. Die Widerstandsfähigkeit der Architektur gegenüber dieser Versuchung, die während der Entwicklung beobachtet wurde, ist selbst ein Beitrag, den dieser Artikel dokumentiert.

Die Vorlagenfamilie ist betriebsbereit: Konfigurationen vom Typ „Village“ laufen auf Infrastruktur unter EU-Hoheitsgewalt (OVH France) und neuseeländischer Hoheitsgewalt (Catalyst Cloud). Spezifische Subdomain-Namen von Mandanten werden in diesem Artikel nicht aufgeführt und wurden absichtlich unkenntlich gemacht, um die Angriffsfläche zu verringern; sie stehen legitimen Gutachtern auf direkte Anfrage beim korrespondierenden Autor zur Verfügung. Jede derzeit betriebsbereite Konfiguration vom Typ „Village“ authentifiziert ihre Mitglieder und gibt eine 302/403-Antwort auf nicht authentifizierte Inhaltsanfragen zurück – das Betriebsmerkmal eines aktiven Mandanten. Eine Carpool-Konfiguration wird derzeit auf der neuseeländischen Infrastruktur als erste geplante Multi-Instanz-Föderationsbereitstellung aufgebaut; Carpool isoliert Föderations- und Verwaltungs-Backend-Primitive ohne die vollständige, mitgliederorientierte Oberfläche anderer Village-Typen, was es zur klarsten pädagogischen Darstellung des Föderationsprimitivs macht. Die Einladung an Gemeinschaften oder Organisationen, die an einer Pilotteilnahme interessiert sind, findet sich in §7.4.

Dorftyp	Zweck (eine Auswahl möglicher Anwendungen)
Whānau	Websites der Māori-Großfamilien mit genealogischem und mündlich überliefertem Material über mehrere Generationen; die auf dem Te Tiriti basierende Souveränität über Inhalte ist strukturell verankert, nicht nur ein Zusatz
Rūnanga	Websites von Iwi-Räten (Stammesräten) mit Protokollen, Ausschussbeschlüssen und Taonga-Beschreibungen, die direkt die Rechte aus dem Te Tiriti betreffen; Austausch zwischen Iwi durch bilaterale Föderation, keine plattformweite Offenlegung
Ausschuss	Beratungsgremien für Sportverbände, Berufsverbände und lokale Vereine, bei denen die Herkunft von Entscheidungen eine Rolle spielt – die signierte Beweiskette des Beratungsinhaltsmodells ist genau dafür ausgelegt
Kāhui Māori	Multi-Iwi-Koordinationsseiten, auf denen der Austausch über bilaterale Verbände zwischen souveränen Iwi-Instanzen erfolgt; jeder Iwi behält die volle Autorität; Verbandsprimitive sind die architektonische Lösung
Governance	Institutionelle Gremien (Gemeinderäte, Schulbehörden, Pfarrgemeinderäte), die sowohl Aufgaben für alle Mitglieder (Protokolle, Beschlüsse) als auch vertrauliche Aufgaben (Mitgliedschaft, Entwürfe, Ausschussberatungen) wahrnehmen – die „Share-within“-Richtlinie mit gruppenweiter Durchsetzung ermöglicht es, beides auf einer einzigen Plattform abzuwickeln

Dorftyp	Zweck (eine Auswahl möglicher Anwendungen)
Mitgliedschaft	National angegliederte Gremien mit lokalen Zweigstellen – ein nationaler Verband, dessen Zweigstellen ihre eigene Mitgliederliste und ihren eigenen Veranstaltungskalender benötigen, verbunden mit dem nationalen Gremium für umfassendere Interaktionen; die vorherrschende Struktur für europäische *Vereine*, Sportverbände, Berufsverbände und Gewerkschaften

Die hier entwickelte Typologie lässt sich über die „Village“-Typen hinaus auf eine breitere Klasse von Organisationsformen verallgemeinern, deren strukturelle Interessen nicht individuell, sondern kollektiv vertreten werden. Sektorale Mitbestimmungsgremien in Rechtsordnungen, in denen Tarifverhandlungen verfassungsrechtlich verankert sind – Betriebsräte nach dem Mitbestimmungsgesetz in Deutschland, Arbeitnehmervertretungen nach dem österreichischen Arbeitsverfassungsgesetz, der belgische „conseil d'entreprise“, skandinavische „samarbejdsudvalg“-Regelungen – sind organisierte Formen, deren Interessen an Datenhoheit nicht allein durch die Rechte einzelner betroffener Personen erfüllt werden. Genossenschaften, in denen die Mitgliedschaftsrechte gleichberechtigt sind und Entscheidungen von Mitgliederversammlungen getroffen werden, haben dieselben architektonischen Anforderungen: bilaterale Verbände zwischen Genossenschaften in verschiedenen Rechtsordnungen; souveräne Datensätze mit mitgliederorientierter Portabilität; eine Stakeholder-Governance-Benutzeroberfläche, die kollektive Beratungen unterstützt. Gewerkschaften in Rechtsordnungen, in denen die gewerkschaftliche Vertretung institutionell verankert ist, weisen dieselbe Struktur auf. Die Architektur schreibt keine bestimmte Governance-Form vor; sie legt die Grundelemente offen, die eine solche Form erfordert.

Weitere Dorf-Typen in der Vorlagenfamilie – Familie (genealogieorientiert), Gemeinde (lokale Kirchengemeinde), Unternehmen (Mitgliederverzeichnis plus Mitteilungen für kleine Händlerverbände) und Fahrgemeinschaft (Mitfahrzentrale, in Entwicklung, Träger des geplanten ersten Multi-Instanz-Verbund-Einsatzes) – sind konkrete Instanzen derselben Vorlagenfamilie. Die Menge ist keine feste Liste; der Wert der Vorlage liegt gerade darin, dass zusätzliche Dorf-Typen ohne architektonische Änderungen konfiguriert werden können.

11.1 Situationsbezogene Sprachschicht-Kohorten (Vorabverweis auf Paper B)

Jede Dorf-Typ-Konfiguration ist mit einer *situierten Sprachschicht-Kohorte* gepaart – einem sprachlichen Modell pro Mandantentyp, das unter strenger Trainingsdisziplin auf den eigenen Inhalten des Mandanten trainiert wurde. Kohorten werden für die derzeit in Produktion befindlichen Dorf-Typen bereitgestellt; designierte Kohorten für zusätzliche Dorf-Typen warten gemäß der Projektdisziplin gegen ambitioniertes Training auf den ersten Mandanten jedes Typs, bevor sie in Betrieb genommen werden. Die empirischen Ergebnisse – einschließlich einer dokumentierten Reihe von Experimenten zur Gewichtsanpassung, die eine einheitliche Verschlechterung zeigen, der vier „No-X"-Regeln zur Hygiene der Trainingsdaten, der CPU-Fallback-Inferenzarchitektur und der Bewertungsergebnisse pro Kohorte – werden separat in der Zusammenfassung von Paper B berichtet.

Auf Plattformebene ist ein Pre-Launch-Gate eingerichtet: Die Erstellung von Mandanten wird bis zur ausdrücklichen Autorisierung durch den Betreiber blockiert. Die Plattform startet Mandanten nicht im Hintergrund; die Sperre stellt sicher, dass jeder operative Mandant einen Autorisierungsschritt durchlaufen hat, der selbst im Audit-Protokoll erfasst wird. Eine separate Sperre für die Souveränitätskonstitution erzwingt einen harten 403-Zugriffsverweigerungsstatus für Mandanten, die nach dem 01.05.2026 erstellt wurden und denen erforderliche Souveränitätsabschnitte fehlen; diese Sperre ist mit integrierter Suspendierungsimmunität für bestimmte Plattform-Infrastruktur-Mandanten in Betrieb.

---

12. Bewertung

Dieser Abschnitt fasst die Belege für die Implementierung der Architektur in einem einzigen Abschnitt zusammen. Es werden drei Ledger und eine Fallstudie vorgestellt: das Use-Case-Verifizierungs-Ledger, das Framework-Konsultations-Ledger, der Deployment- und Verifizierungs-Snapshot sowie die Fallstudie zur Hash-Stabilität im Hydration-Modus vom 22.04.2026.

12.1 Versuchsaufbau

Die Plattform läuft in der Produktion an zwei Infrastrukturstandorten: einer EU-souveränen Bereitstellung bei OVH France (community.myfamilyhistory.digital und zugehörige Mandanten-Subdomains unter mysovereignty.digital und myfamilyhistory.digital) und einer neuseeländisch-souveränen Bereitstellung auf Catalyst Cloud (village-nz-Infrastruktur unter 202.49.243.176, die die mysovereignty.digital-Tenant-Subdomains bedient). Beide Standorte führen denselben Code in derselben Revision aus; die Spiegelparität wird über zwei Bereitstellungsziele sowie einen selbst gehosteten Forgejo-Upstream

hinweg aufrechterhalten. Die Datenbank ist standortbezogen MongoDB mit mandantengebundenen Abfragen, die durch ein Mongoose-Plugin erzwungen werden; die Laufzeitinferenz für die situierte Sprachschicht wird auf einer neuseeländischen GPU gehostet (Catalyst A6000 während der Geschäftszeiten, Heim-eGPU außerhalb der Geschäftszeiten) mit automatischem Failover.

12.2 Verifizierung des Anwendungsfalls Ledger

Das Anwendungsfall-Ledger zeigt, dass jede implementierte Komponente wie vorgesehen mit einer lokalen Live-Datenbank arbeitet. Das Ledger deckt die architektonischen Komponenten ab: Kanonisierung der Provenienz; die Policy Inheritance Engine und ihre Filtermodi; Verifizierungs-Caching; Proof-Chain-Signierung einschließlich UPDATE und DELETE im Abfragemodus; den Governance-Queue-Tombstone-Pfad; DID-Veröffentlichung; den Export-Wrapper einschließlich des Sichtbarkeits-Overlays; konstitutionelle Voraussetzungen; die Föderationsoberfläche; die Migration souveräner Datensätze über die vom Mandanten generierten Inhaltsmodelle hinweg und die Abdeckung eingebetteter Unterdokumente; Gruppenbereichs-Verkabelung einschließlich der Chat-Thread-Oberfläche; DSR-kanonische Export- und Ingest-Pfade; Worker-Policy-Abgleich; WebSocket-Policy- Anpassung; Tombstone-Nachrüstung; Proof-Chain-Komprimierung; die Access-Gate- Oberfläche; die mandantenbezogenen Viewer-Seiten. Die PASS-Rate des Ledgers liegt zum Snapshot-Zeitpunkt auf Parität; der Skriptsatz ist durch einen externen Prüfer mit Zugriff auf die Codebasis reproduzierbar (Anhang B fasst die Kategorien zusammen).

12.3 Framework-Konsultations- Ledger

Das Ledger zur Rahmenkonsultation erstreckt sich über die gesamte Architektur. Jeder Datensatz nennt den konsultierten Dienst, das Urteil pro Bedingung und die operativen Metadaten (Operationsname, Dauer, Ergebnisklasse). Der Satz der aktiven Dienste deckt die Kern-Tractatus-Dienste ab (BoundaryEnforcer, ContextPressureMonitor, MetacognitiveVerifier, PluralisticDeliberationOrchestrator, CrossReferenceValidator, InstructionPersistenceClassifier) sowie eine breitere Palette entscheidungsspezifischer Dienste, die im Zuge des Wachstums der Architektur hinzugekommen sind (TractatusAuditRecorder, SovereigntyPrimacyEnforcer, PolicyCoherenceValidator, TenantIsolationValidator, AuditTrailVerifier, SchemaGuardian, PolicyDecisionOracle, TenantOwnerAuthority, PluralisticDeliberator, GovernanceOrchestrator). Das Ledger wird einheitlich in lokalen sowie in EU- und neuseeländischen Produktionsdatenbanken gespeichert – drei Eintragsorte pro Konsultation –, sodass der Ausfall eines einzelnen Hosts die Audit-Position nicht gefährdet. Ein planmäßiger Zustandscheck meldet die Aktualität der Konsultationen pro Dienst anhand von Schwellenwerten, die auf realistische Arbeitsrhythmen abgestimmt sind (systemweit 4 Stunden, 24 Stunden pro Dienst); diese Schwellenwerte ersetzten frühere 30-Minuten-Standardwerte, die falsch-positive Fade-Warnungen bei jeder kurzen Unterbrechung der aktiven Entwicklung auslösten.

12.4 Bereitstellungsmetriken

Bereitstellungsstatus zum Zeitpunkt des Snapshots: Beide Produktionsstandorte melden `/api/health` 200; die Dienste des Framework-Moduls melden „operational“ auf beiden Standorten; „verify-and-cache“ läuft nächtlich über die vom Mandanten generierten Inhaltsmodelle; die Catalyst-Smoke-Test-Oberfläche (catalyst-operational) besteht bei voller Abdeckung; ESLint läuft fehlerfrei über die geänderten Dateien bei jedem Deployment; die Spiegelparität wird über `ovh`, `catalyst` und `forgejo` hinweg aufrechterhalten. Das während aktiver Wartungsfenster beobachtete Smoke-Test-Ergebnis „FAIL“ ist erwartetes Verhalten – der Smoke-Test fragt Produktions-Endpunkte ab, die während der Sperre Wartungs-HTML bereitstellen – und wird wieder auf „PASS“ gesetzt, sobald das Wartungsfenster aufgehoben ist.

12.5 Beobachtbarkeit des Verifizierungs-Caches

Der Verifizierungscache wird über den operativen Mandantensatz auf beiden Produktionsstandorten gefüllt und umfasst die elf derzeit aktiv genutzten Inhaltstypen. Datensätze ohne Provenienz-Hash (ein kleiner Restbestand an Altdatensätzen aus der Zeit vor der Migration zu Sovereign-Datensätzen) werden als `„unverifizierbar"` statt als `„gültig"` gekennzeichnet. Die architektonische Eigenschaft besteht darin, dass das Verifizierungsfeld in jeder API-GET- Antwort den Cache-Status für Verbraucher sichtbar macht; nachgelagerte Audit-Tools können den Verifizierungsstatus der Architektur durch Abfrage der API-Oberfläche ermitteln, ohne dass ein Datenbankzugriff erforderlich ist. Der wesentliche Beitrag liegt in der Observability-Disziplin, nicht in der Anzahl der Datensätze.

12.6 Fallstudie: Der Hash-Stabilitätsfehler im Hydration-Modus vom 22.04.2026

Das lehrreichste empirische Ereignis während der Entwicklung der Architektur war die Entdeckung eines Hash-Stabilitätsfehlers während der Anwendungsfall-Validierung der Read-Path-Integration des Verifizierungs-Caches. Der Serializer für die kanonische Form durchlief die enumerierbaren Eigenschaften eines ORM-Unterdokuments – ein Muster, das bei Payloads mit einfachen Objekten korrekt funktionierte, bei hydrierten Dokumenten jedoch den internen ORM-Zustand offenlegte und Hashes erzeugte, die je nach Hydrationsmodus voneinander abwichen. Hashes zur Speichersicherung zwischenspeicherten einen Wert; Hashes zur Lesezeit berechneten einen anderen; jeder Datensatz nach der Bereitstellung würde `einen „chain_hash_mismatch"` aufweisen. Die Behebung bestand aus einem einzeiligen Normalisierungsschritt. Der Fehler hatte die Unit-Test-Suite einwandfrei bestanden, da die Tests Einträge mit einfachen Objekten simulierten – der Fehlermodus erforderte echte hydrierte Dokumente.

Dies ist ein tragendes Beispiel für die Betriebsdisziplin: Tests beweisen, dass die Verkabelung in Mocks funktioniert, aber die Use-Case-Validierung gegen

eine Live-Datenbank beweist, dass die Verkabelung in der Realität funktioniert. Die Disziplin, dass Tests beweisen, was Mocks offenbaren, und dass die Use-Case-Validierung aufzeigt, was Mocks verbergen, ist in der Betriebsdisziplin des Projekts verankert und ist der Grund, warum neben der Unit-Test-Suite ein Use-Case-Validierungsskriptsatz existiert. Nach der Behebung wurden alle vorhandenen Produktionsdatensätze mit dem korrigierten Serializer für die kanonische Form erneut zwischengespeichert; es ging kein Datensatz verloren, keine Audit-Position wurde beeinträchtigt, und der Fehler ist das kanonische Beispiel, das in der Schulung zur Betriebsdisziplin verwendet wird.

12.7 Interpretation

Die Bewertungsergebnisse stützen eine konkrete Behauptung: Die Architektur ist an der API-Oberfläche über mehrere souveräne Infrastrukturstandorte hinweg betriebsbereit, beobachtbar und überprüfbar. Die Verifizierungsoberfläche (Use-Case-Ledger, Framework-Consultation-Ledger, Bereitstellungsmetriken) ist für jeden Prüfer mit Zugriff auf den Code reproduzierbar; die Fallstudie zur Hash-Stabilität zeigt, dass die Betriebsdisziplin reale Fehlermodi erfasst, die von Mock-Tests übersehen werden. Was die Bewertung *nicht* behauptet, ist, dass jede Bedrohung in §4 umfassend abgewehrt wird – die Architektur verteidigt *benannte* Invarianten mit *benannten* Prädikaten; Bedrohungen außerhalb des Modells (Angriffe durch abstreitbare Verschlüsselung; Kompromittierung der Lieferkette des Frameworks Tractatus; physische Kompromittierung der Hardware der Inferenzschicht) liegen außerhalb des Geltungsbereichs und werden in der Betriebsdisziplin als separate Themen verfolgt.

---

13. Open-Source-Haltung

Die Open-Source-Haltung unterscheidet zwei Stränge.

Das **Tractatus-Framework** – der Mechanismus zur Steuerung der Entwicklungsphase – ist öffentlich, unter der Apache 2.0-Lizenz als Open Source verfügbar und wird unter `codeberg.org/mysovereignty/tractatus-framework` [1] bereitgestellt. Sein Arbeitspapier, seine Codemuster und Metriken sind von einem externen Prüfer reproduzierbar, der Zugriff auf eine Installation der Klasse „Claude-Code“ und die Musterbibliothek des Frameworks hat.

Der Code der Plattform – die Laufzeitanwendung – wird modulweise als Open-Source-Version unter der European Union Public Licence Version 1.2 (EUPL-1.2) [10] veröffentlicht. Die Quelldateien enthalten pro Datei EUPL-1.2-Kopfzeilen; die zuletzt geänderten Dateien der Plattform (Provenienz, Verifizierungs-Cache, Gruppenbereichs-Attribution, Hooks für Lösch- und Aktualisierungsvorgänge im Abfragemodus, kanonischer DSR-Export, Föderationsdienste, UI-Komponenten für Stakeholder, Worker-Policy-Helfer) tragen den Header. Die Lizenz auf Repository-Ebene steht noch aus, bis eine Governance-Gesellschaft nach neuseeländischem Recht mit einem

demokratisch gewählten Vorstand und einem Beirat gegründet ist. Der Vorstand genehmigt architektonische Änderungen, die Auswirkungen auf die Open-Source-Ausrichtung der Plattform und die Verpflichtungen der Stakeholder haben; der Beirat bietet kulturelle und stakeholderbezogene Beratung (Māori- Kulturberatung; Beratung für Minderheitensprachen-Communities; FOSS-Community- Beratung). Der Vorstand wurde noch nicht konstituiert; die EUPL-1.2-Header pro Datei sind die derzeitige Open-Source-Vorbereitung, nicht der endgültige Zustand auf Repository-Ebene.

Der Release-Pfad „Modul für Modul“ wurde bewusst einer vollständigen Repository-Veröffentlichung vorgezogen. Der ausschlaggebende Grund ist eine Klasse von Angriffsflächen bei großen Sprachmodellen, bei der eine vollständige Quellcode-Veröffentlichung einer intern gekoppelten Plattform Material offenlegt, dessen Bedrohungsmodell an der Modulgrenze noch nicht überprüft wurde – Code, der nur bestimmten Angriffen widersteht, weil er noch nicht von Modellen gelesen wird, die auf feindlichen Korpora trainiert wurden. Eine sorgfältige Veröffentlichung auf Modulbasis ermöglicht es, das Bedrohungsmodell Eine sorgfältige Veröffentlichung auf Modulebene ermöglicht es, das Bedrohungsmodell jedes Moduls vor der Veröffentlichung zu überprüfen, und begrenzt das Überschwappen interner Kopplungen auf extern abhängige Oberflächen. Die bisher veröffentlichten Module – das Kern-Plugin für souveräne Datensätze, die Policy Inheritance Engine, der Tenant-Schlüsselspeicher, das Tractatus-Framework sowie Komponenten der DSR- Pipeline – bilden die architektonische Oberfläche, auf die externe Prüfer zugreifen können; nachfolgende Module folgen dem gleichen Rhythmus von Überprüfung und Veröffentlichung.

Ein Entwurf der „Village Model Licence“ liegt als benutzerdefinierte Lizenzform vor, die darauf abzielt, FOSS-typische Berechtigungen mit spezifischen Klauseln zum Schutz der Community zu kombinieren (keine Nutzung zur Überwachung von Communities; keine Nutzung, die gegen die Datenhoheitsbestimmungen einer Community verstößt; keine Nutzung, die die erklärte Haltung eines Mandanten zu den CARE-Prinzipien umgeht). Der Entwurf wartet auf eine formelle rechtliche Prüfung; bis zum Ergebnis der Prüfung bleibt die dateibasierte Lizenzierung der Plattform EUPL-1.2.

13.1 Anbieter-Disziplin

Die Plattform nutzt in ihrem Produktionsanforderungsweg keine US-amerikanischen Cloud-, SaaS- oder Infrastruktur- Abhängigkeiten. Das EU-souveräne Hosting erfolgt bei OVH France; das neuseeländisch-souveräne Hosting bei Catalyst Cloud (mit Catalyst (NZ) Limited als juristischer Person); das Home-eGPU-Failover für Inferenz außerhalb der Geschäftszeiten erfolgt auf einer nicht-US-amerikanischen Grafikprozessoreinheit. Das Hosting des Code-Repositorys ist aufgeteilt: Eine selbst gehostete Forgejo-Instanz ist der EU-souveräne primäre Remote-Server, mit Spiegeln zu den Bare-Repositorys von OVH und Catalyst. Die Zahlungsabwicklung erfolgt über Airwallex (NZ)

Limited – US-Kreditkartennetzwerke werden nur pro Transaktion genutzt, wenn der Kartenaussteller des Zahlers in den USA ansässig ist, und nur für diese einzelne Transaktion. Als Übersetzungstool wird DeepL (deutsches Unternehmen, unterliegt der EU-DSGVO) verwendet. Diese Anbieterregelung wird durch eine interne Richtlinie durchgesetzt, die zulässige und unzulässige Anbieter ausdrücklich auflistet; Abweichungen erfordern eine ausdrückliche Entscheidung auf Projektebene, keine stillschweigende Einführung.

Es werden keine biometrischen Daten von der Plattform erfasst. Die Identitätsprüfung von Mitgliedern bei risikoreichen Vorgängen erfolgt außerhalb des Systems (persönliche Vorstellung innerhalb der Community; Videovorstellung; Überprüfung auf Papier) oder über den vom Mitglied kontrollierten Signaturschlüssel für dezentrale Identifikatoren, niemals über biometrische Erfassung. Die Begründung ist struktureller Natur und ergibt sich aus vier Aspekten: Biometrische Daten sind unwiderruflich, sodass ein Datenleck nicht durch Rotation behoben werden kann; biometrische Daten weisen drei strukturelle Wege auf, über die sie der US-Gerichtsbarkeit ausgesetzt sind (direkte Erfassung durch die USA an Grenzen und bei Visumsgesprächen; Hosting in US-Clouds, das dem dem Zwang des CLOUD Act unterliegt, unabhängig von der Staatsangehörigkeit der betroffenen Person; künftige Vereinbarungen im Rahmen der „Enhanced Border Security Partnership“, die einen direkten Datenbankzugriff auf biometrische Repositorien von Partnerländern vorsehen); biometrische und DNA-Daten der Māori unterliegen einem spezifischen Schutz gemäß Te Tiriti / WAI 262 / WAI 2522 Schutz, der wirksam wird, sobald solche Daten auf der Plattform erfasst werden, und die Weitergabe dieser Daten durch die Krone an eine ausländische Rechtsordnung stellt den Schutz von Taonga gemäß Artikel 2 in einer Weise auf die Probe, die die Plattform nicht ausschließen darf; und die ergonomischsten biometrischen Anwendungsprogrammierschnittstellen werden von Unternehmen mit Sitz in den USA betrieben, deren Nutzung in jedem Fall gegen die Anbieter-Verbotsregel der Plattform verstoßen würde. Die Weigerung, biometrische Daten zu erheben, entzieht die Plattform architektonisch dieser gesamten Risikofläche – der Betreiber kann nicht gezwungen werden, etwas offenzulegen, das nie erhoben wurde. Mitglieder, die eine gerätelokale biometrische Entsperrung ihres eigenen Zugangsdaten-Tresors nutzen möchten, können dies auf ihrer eigenen Hardware tun; die biometrischen Daten überqueren niemals die Grenze der Plattform, und die Plattform greift nicht in dieses Muster ein. Die eigene Zugriffsfläche der Plattform – einschließlich des mitgelieferten Sovereign Access Gate (§15), dessen Aktivierung pro Mandant vom Betreiber gesteuert wird – nutzt Text-Passphrasen (Dice-Words / im Stil der EFF-Wortliste; hohe Entropie und rotierbar) sowie selbst gehostete Proof-of-Work- Bot-Erkennung.

13.2 Der IP-Perimeter

Die Veröffentlichungsstrategie unterscheidet die *architektonische Form* (veröffentlichbar als Artikelinhalt; veröffentlicht als Open-Source- Module) von

den *betrieblichen Einzelheiten* (zurückgehalten aus Gründen des IP- Perimeters). Zurückgehalten: spezifische Tractatus-Framework-Abfragebedingungen pro Dienst (der Katalog ist der Beitrag des Frameworks); Vokabularinhalte pro Produkttyp, die über die übergeordnete Vorlagenfamilie hinausgehen; konfigurationsspezifische Details pro Mandant; spezifische Details zu Feldsätzen im Föderationsmanifest, die über die architektonische Form in Anhang C hinausgehen. Veröffentlicht: die architektonischen Primitive im Artikel; das Bedrohungsmodell und testbare Prädikate; die übergeordneten Schemaformen; die Einschränkungen und Ausfallmodi (§15); die Quellmodule gemäß dem modulweisen Veröffentlichungsplan.

---

14. Der architektonische Beitrag

Die Architektur ist eine Antwort auf eine strukturelle Gegebenheit, kein konkurrierendes Produkt. Das Standardmodell der Community-Plattform – in US-Besitz, aufmerksamkeitsorientiert, mit nach Belieben revidierbaren Nutzungsbedingungen – ist eine bestimmte architektonische Entscheidung darüber, wo die Datenhoheit liegt. Eine architektonische Entscheidung kann nur durch eine architektonische Alternative beantwortet werden, nicht durch Änderungen der Nutzungsbedingungen oder Funktionserweiterungen bestehender Plattformen.

Vier Eigenschaften der Arbeit spielen dabei eine Rolle.

Die Arbeit ist **betriebsbereit**. Die Architektur ist keine Spezifikation, die auf ihre Umsetzung wartet. Sie läuft bereits in mehreren dorfartigen Konfigurationen auf Infrastruktur unter der Hoheit der EU und Neuseelands. Ein Prüfer kann den Betriebsstatus über die API-Oberfläche überprüfen und jede architektonische Entscheidung über das persistente Framework-Konsultations-Ledger verifizieren. Das Use-Case-Verifizierungs-Ledger deckt die implementierte Architekturoberfläche vollständig ab. Der wesentliche Beitrag liegt in der Disziplin der Aufzeichnung – dass die Architektur Audit-Artefakte erzeugt, die von außen beobachtbar sind, ohne dass man dem Wort des Betreibers vertrauen muss.

Die Arbeit ist **strukturell übertragbar**. Die Architektur geht nicht speziell von Māori-Gemeinschaften, Te Reo Māori oder Te Tiriti aus. Dasselbe Feld `„metadata.origin.collective_id"`, das es einer Māori-Gemeinschaft ermöglicht, einen Datensatz ihrer Rūnanga zuzuordnen, ermöglicht es einer walisische Gemeinschaft einen Datensatz ihrer Gemeinde zuordnen, eine samische Gemeinschaft ihrer Siida und eine sorbische Gemeinschaft ihrem Dorf. Das Muster der situierten Sprachschicht ist ähnlich portabel: Eine walisischsprachige Schicht, die auf walisischsprachigem Material unter der Aufsicht der walisischen Gemeinschaft trainiert wurde, beantwortet walisische Anfragen mit derselben architektonischen Haltung, wie die maorischsprachige

Schicht maorische Anfragen beantwortet. Die Architektur ist ein Substrat, kein Produkt.

Das Projekt ist **föderationsfähig**. Die Infrastruktur für bilaterale Föderationen wird End-to-End ausgeliefert, einschließlich einer umfassenden Negativtestmatrix, die Umfang, Schreibsperren, Audit, Zitierdisziplin, Caching, Randfälle, Autorisierung und Phase-3-Namensraumtrennung abdeckt. Live-Föderationsverbindungen zwischen unabhängigen Mandantenbereitstellungen stehen erst nach der ersten Multi-Instanz-Bereitstellung zur Verfügung; die architektonische Eigenschaft – dass zwei Gemeinschaften sich zu von ihnen festgelegten Bedingungen auf eine bestimmte, begrenzte Interaktion einigen können, und nur darauf – ist genau das, was die drei Artikel von Te Tiriti für die digitale Infrastruktur implizieren und was Minderheitensprachgemeinschaften in Europa benötigen, wenn ihre gemeinschaftsübergreifende Arbeit rechtliche Zuständigkeiten überbrückt.

Die Arbeit **respektiert die Portabilität**. Ein Mitglied ist ein vollwertiger Datensubjekt. Es kann seinen vollständigen Datensatz in kryptografisch überprüfbarer Form exportieren und zu jedem anderen Mandanten migrieren, der unter demselben Architekturmodell betrieben wird. Der Export entspricht dem Auskunftsrecht gemäß Artikel 15 der DSGVO; die Migration entspricht der architektonischen Verpflichtung, dass der Austritt eine vollwertige Operation ist. Ein Community-Modell, bei dem der Austritt schwierig ist, ist ein geschlossener Garten, unabhängig von der verwendeten Marketing-Sprache; ein Community-Modell, bei dem der Austritt architektonisch verankert ist, ist das, was die hier vorgestellte Arbeit ermöglicht.

Der wesentliche Anspruch der Architektur besteht darin, dass eine Plattform im Gemeinschaftsmaßstab so aufgebaut werden kann, dass ihre Souveränitätsgarantien auf der Ebene der Datensätze und der Mandanteninfrastruktur bestehen, nicht im Ermessen des Betreibers. Das Standardmodell beruht auf einer vom Betreiber gewährten und vom Betreiber widerrufbaren Souveränität; eine architektonische Alternative – Souveränität als Eigenschaft der Datensätze und der Mandanteninfrastruktur – lehnt diese Bedingung konstruktionsbedingt ab. Die hier vorgestellte Arbeit ist ein Praxisbeispiel dafür, dass eine solche Alternative von einem kleinen Team in Neuseeland mit geringem Budget aufgebaut und in der Produktion für echte Gemeinschaften betrieben werden kann, selbst wenn sich das regulatorische Umfeld weiterhin in Richtung einer Durchgriffsmöglichkeit ausländischer Gerichtsbarkeiten bewegt (wobei die Enhanced Border Security Partnership das aktuelle Beispiel in Neuseeland ist).

---

15. Einschränkungen und Fehlermodi

Mehrere Punkte fallen in den Geltungsbereich der Aussagen dieses Artikels, sind jedoch zum Zeitpunkt dieses Entwurfs noch nicht implementiert:

- **Live-Verkehr der Carpool-Föderation.** Die bilaterale Föderationsinfrastruktur wird End-to-End mit einer umfangreichen Verifizierungsfläche ausgeliefert, jedoch wurde noch keine Live-Föderation zwischen unabhängigen Tenant-Bereitstellungen aktiviert. Die Carpool-Föderationsbereitstellung, die als erstes Multi-Instanz-Beispiel vorgesehen ist, erfolgt im Tempo des Betreibers.
- **Tier-2-Kohorten auf der situierten Sprachschicht.** Designierte Kohorten für zusätzliche Dorf-Typen werden gemäß der Projektdisziplin gegen ambitioniertes Training pausiert: Eine Kohorte wird erst in Betrieb genommen, wenn der erste Mandant dieses Typs im Einsatz ist.
- **Vollständige Open-Source-Veröffentlichung auf Repository-Ebene.** Die EUPL-1.2-Header der Plattform auf Dateiebene sind vorhanden; die modulweise Veröffentlichung läuft; die Lizenz auf Repository-Ebene steht zur Genehmigung durch den Vorstand aus, und der Vorstand selbst steht unter neuseeländischem Recht zur Gründung als Körperschaft aus.
- **Veröffentlichung der Tiriti-Konformitätserklärung v0.2.** Eine Revision v0.2 existiert nach bestem Ermessen des vom Betreiber beauftragten Vertreters; die namentliche Veröffentlichung erfordert die ausdrückliche Zustimmung von Dr. Taiuru.
- **Formelle rechtliche Prüfung der Village Model Licence.** Der Entwurf liegt vor; die formelle rechtliche Prüfung steht noch aus; bis zum Vorliegen des Ergebnisses bleibt die Lizenzierung der Plattform auf Dateiebene EUPL-1.2.
- **Identitätsabgleich für empfangende Mandanten und automatisches Onboarding.** Der aktuelle DSR-Migrationspfad lehnt das automatische Onboarding standardmäßig ab; das automatische Onboarding über mandantenübergreifende DIDs ist eine Sicherheitsfläche, die eine eigene Designüberprüfung erfordert.
- **Souveränes Zugangstor (Passphrase + souveräner Proof-of-Work Bot-Erkennung + Papier-Wiederherstellungscodes) – ausgeliefert, mandantenweiser Rollout im Tempo des Betreibers.** Die Basisauthentifizierung der Plattform besteht aus httpOnly-Cookies sowie einer auf der Datenbankabfrageebene erzwungenen Mandantenkontext-Isolierung. Die Access-Gate-Komponente wird durchgängig als globale Request-Pipeline-Middleware (`accessGate`) mit einer mandantenbezogenen `AccessGateConfig` (Passphrase-Hash, Rotationsverlauf, Anzahl der Wiederherstellungscodes) und zehn REST-Endpunkten (`/api/access-gate/{status, pow/{challenge,verify}, passphrase/verify, recovery/use, admin/{enable,disable,rotate,status,recovery-codes/pdf`
einem selbst gehosteten Proof-of-Work-Challenge/Verify-Paar (kein Bot-Erkennungsdienst von Drittanbietern) und ausdruckbaren Wiederherstellungscodes, die auf PDF auf Anfrage des Betreibers generiert werden (keine SMS, keine E-Mail, kein Out-of-Band-Kanal, der über US-Infrastruktur geleitet wird). Die Komponente ist standardmäßig bei jedem Mandanten deaktiviert; die mandantenweise Einführung – Ausgabe von Passphrasen,

Verteilung von Wiederherstellungscodes , Onboarding von Mitgliedern in das Gate – erfolgt im Tempo des Betreibers und läuft mandantenweise unter dokumentierter Überprüfung ab. Die architektonische Verpflichtung zu einer rein textbasierten und biometriefreien Authentifizierung, wie sie in §13.1 zur Anbieterdisziplin und in §4 zur unveränderlichen I9 festgeschrieben ist, ist dauerhaft und wird heute durch die bestehende Haltung der Plattform, keine biometrischen Daten zu erheben, durchgesetzt, unabhängig vom Stand der mandantenweisen Einführung des Gateways. Architektonische Ausschlüsse, die sich explizit auf das Design des Zugangstors beziehen – biometrische Authentifizierung, SMS-basierte Zwei-Faktor-Authentifizierung, E-Mail-Magic-Links über in den USA gehostete Anbieter, von den USA kontrollierte Push-OTP, von den USA kontrollierte Bot-Erkennungsdienste, verhaltensbasierte Biometrie – sind im zugelassenen Plan des Zugangstors mit der Begründung dokumentiert, die jedem Ausschluss zugrunde lag, sodass die Auswahlmöglichkeiten dauerhaft festgelegt sind und nicht dem Zufall überlassen bleiben. Was weiterhin vom Betreiber bestimmt wird, ist die Entscheidung über die Aktivierung pro Mandant, nicht die Existenz der Komponente.

- **Rechtspersönlichkeit von KI-Agenten – offene Frage, behandelt in Paper B.** Dr. Taiuru (2026) [25a] wirft als offene Frage auf, ob und unter welchen Bedingungen die Rechtspersönlichkeit auf KI-Agenten ausgeweitet werden könnte, die auf Māori-Wissen basieren, und verweist die Entscheidung ausdrücklich an die gemeinsame Arbeit von KI-Entwicklern, Behörden und Māori-Gemeinschaften. Das Begleitpapier B berichtet über die Disziplin des kohortenbezogenen Trainings auf der situierten Sprachebene, auf die sich jede zukünftige partnerschaftliche Arbeit pro Kohorte stützen würde; dieses Papier greift dieser Arbeit nicht vor oder beurteilt sie vorzeitig.

Bedrohungen außerhalb des §4-Modells werden in der Betriebsdisziplin separat verfolgt: Angriffe mit abstreitbarer Verschlüsselung gegen den Schlüsselspeicher; Kompromittierung der Lieferkette des Tractatus-Frameworks oder seiner Abhängigkeiten; physische Kompromittierung der Hardware der Inferenzschicht; Veralterung kryptografischer Primitive außerhalb der Reichweite des Algorithmus-Agility-Wrappers. Keine dieser Bedrohungen wird in diesem Artikel behandelt; alle stellen reale Bedenken auf der Implementierungsebene dar und erfordern eigene Analysen.

Zwei strukturelle Einschränkungen sind eher systemimmanent als implementationsbedingt. Die Architektur bewahrt die Souveränität der Gemeinschaft über Daten; sie bewahrt jedoch nicht an sich die Souveränität der Gemeinschaft über *die Kognition*. Eine Gemeinschaft, die die Situated-Language-Schicht zur Vermittlung von Mitgliederanfragen nutzt, verwendet nach wie vor ein Sprachmodell; der Trainingskorpus, die Trainingsdisziplin und das Laufzeitverhalten des Modells sind Teil der Architektur und nicht von ihr getrennt. Papier B wird die empirische Trainingsdisziplin dokumentieren,

die die Situationssprachsschicht für die Nutzung durch die Gemeinschaft vertrauenswürdig macht; seine Ergebnisse schränken die Schlussfolgerungen ein, die ein Leser allein aus diesem Papier ziehen kann. Die andere strukturelle Einschränkung besteht darin, dass die Abwehr der Architektur gegen den in §4 genannten Gegner A1 (ein durch Rechtshoheit dazu zwingender Host-Betreiber) letztlich davon abhängt, dass der Mieter seine eigene Infrastruktur betreibt oder eine Partnerschaft mit einem Host unter souveräner Rechtshoheit eingeht: Die Architektur kann keine Souveränität schaffen, wo die Rechtshoheit des Hosts diese nicht unterstützt, aber sie kann die Souveränität für Mieter bewahren, deren Hosts selbst unter souveräner Rechtshoheit stehen.

---

16. Schlussfolgerung

Die hier beschriebene Architektur ist implementiert und läuft auf Infrastrukturen unter EU-Hoheitsgewalt und neuseeländischer Hoheitsgewalt. Ihre Kernprimitiven sind einsatzbereit: Mandantenisolierung als grundlegende Primitive; einheitliche Metadaten für Hoheitsdatensätze über die mandantengenerierten Inhaltsmodelle hinweg; kryptografische Provenienz mit Algorithmusflexibilität; Richtlinienvererbung mit Gating auf Basis der effektiven Richtlinie an der Lese-Grenze; Proof-Chain-Signierung über Erstellungen, Aktualisierungen und Löschungen hinweg (sowohl im Dokument- als auch im Abfragemodus); Verifizierungs-Caching, das zum Zeitpunkt des Lesens auftaucht; mandantenbezogener Schlüsselspeicher mit kryptografischer Löschfinalität; Veröffentlichung dezentraler Identifikatoren; Governance-Warteschlange mit signiertem Entscheidungspfad; Export-Wrapper mit Sichtbarkeitsüberlagerung für Nicht-Administratoren und symmetrischer Audit-Protokollierung; bilaterale Föderation mit signiertem Manifest; mitgliedergeführte souveräne Portabilität mit Artikel-15-symmetrischer Aufnahme durch den empfangenden Mandanten; mandantenspezifische Situations-Sprachschicht; Stakeholder-Governance-Benutzeroberfläche mit schreibgeschützter Überprüfungsoberfläche (Phasen 1–5) sowie die ausgelieferte Phase-6-Oberfläche für den überwachten partizipativen Dialog (vom Betreiber freigegebene redaktionelle Warteschlange, Draft-and-Publish-Gate, keine automatische Veröffentlichung), verallgemeinert über die Produkttypen der Plattform in Phase 7; Angleichung von Worker- und WebSocket-Richtlinien; Proof-Chain-Komprimierungs- Primitiv; Tombstone-Nachrüstungs-Primitiv; und das ausgelieferte souveräne Zugangsgate (Text-Passphrase + selbst gehostete Proof-of-Work-Bot-Erkennung + Papier-Wiederherstellungscodes; Rollout pro Mandant im Tempo des Betreibers).

Das Rahmenkonsultations-Ledger deckt die gesamte Architektur ab (jede Konsultation wird einheitlich in lokalen sowie in EU- und neuseeländischen Produktionsdatenbanken erfasst); das Verifizierungs-Ledger für Anwendungsfälle deckt die implementierten Architekturkomponenten paritätisch ab; die bilaterale Verbundinfrastruktur wird durchgängig mit einer umfassenden Negativtestmatrix ausgeliefert (eine Teilmenge, die zusätzlich von einem Live-

Multi-Tenant-Validator durchlaufen wird), wobei Live-Verbundverbindungen zwischen unabhängigen Mandanten bis zur ersten Aktivierung des Multi-Instanz-Carpools ausstehen; die nach Dorf-Typen gegliederten Kohorten der situativen Sprachschicht sind betriebsbereit; designierte Kohorten für zusätzliche Dorf-Typen warten vor der Inbetriebnahme auf den ersten Mandanten jedes Typs, gemäß der Projektdisziplin im Hinblick auf das angestrebte Training.

Das Begleitpapier (Paper B – Situierte Sprachschichten für Minderheitensprachen und indigene Gemeinschaften, Zusammenfassung des empirischen Begleitartikels, veröffentlicht) beschreibt das Architekturmuster für die Kohorten der situierten Sprachschicht: KI-Systeme pro Gemeinschaftstyp, die auf den eigenen Datensätzen dieser Gemeinschaft trainiert wurden, die Betriebsprinzipien, denen das Projekt beim Training und Betrieb folgt, die heute laufenden Tier-1-Bereitstellungen und die CPU-Fallback-Inferenzarchitektur, die den Laufzeitpfad vollständig außerhalb der von den USA kontrollierten Infrastruktur hält. Das vollständige empirische Papier – mit einer Bewertung pro Kohorte, Ablationen zur Gewichtsmodifikation, einer Literaturrecherche zu Vergleichsstudien und einer eingehenden Auseinandersetzung mit Dr. Taiurus umfassenderem Werk zur KI-Governance der Māori – sowohl dem Kaupapa Māori AI Framework [25b] (die auf dem Te Tiriti basierenden präskriptiven Grundsätze für KI-Einwilligung, Datenhoheit und lückenlose Rechenschaftspflicht) als auch die neuere Untersuchung [25a] (die offene Frage der Rechtspersönlichkeit für KI-Agenten, die auf Māori-Wissen beruhen, die Dr. Taiuru ausdrücklich der gemeinsamen Arbeit von KI-Entwicklern, Regierungsbehörden und Māori-Gemeinschaften überlässt) – wird zurückgestellt, bis verifizierte Trainingsdaten vorliegen. Die vollständige Abhandlung ist der Ort, an dem die beiden von Dr. Taiuru unterschiedenen Ebenen – die präskriptive Governance-Pflicht und die interrogative Frage der Rechtspersönlichkeit – direkten Einfluss auf die hier beschriebene Kohorten-Disziplin nehmen werden. Der vollständige Artikel wird Meads Tikanga-Test (tapu, mauri, take-utu-ea, whanaungatanga) als Bewertungsgrundlage heranziehen, auf die sich jede zukünftige partnerschaftliche Arbeit pro Kohorte stützen würde; er greift dieser partnerschaftlichen Arbeit jedoch nicht vor, sondern wird die Kohorten-Trainingsdisziplin in den empirischen Details darlegen, die eine solche partnerschaftliche Arbeit erfordern würde.

Der Beitrag dient als konkretes Beispiel dafür, wie architektonische Souveränität auf Te Tiriti, KI-Personhood (Dr. Taiuru 2026) und EBSP-klassifizierte Zuständigkeitszwänge im Rahmen des Budgets eines kleinen Teams reagieren kann. Die Architektur ist der Beitrag; die Umsetzung, d. h. die Verpflichtung des entsprechenden Autors, die Architektur unter den von ihr verteidigten Einschränkungen zu betreiben, ist der Beweis. Kommentare und Korrekturen an den korrespondierenden Autor sind willkommen.

Danksagungen

Der Autor dankt Leslie Stroh für die grundlegende philosophische Betreuung zum pluralistischen Denken und zur Frage des Guten in der künstlichen Intelligenz. Das Bekenntnis zur pluralistischen Deliberation, das sich durch die Governance-Architektur der Plattform zieht – und die weitergehende Überzeugung, dass ein KI-Substrat, das es wert ist, aufgebaut zu werden, einem substanziellen Begriff des Guten entsprechen muss, nicht einem prozeduralen – verdankt seine formative Gestalt diesen Gesprächen.

Der Autor dankt außerdem Dr. Karaitiana Taiuru für seine kulturelle Sicherheitsprüfung der Tiriti-Konformitätserklärung v0.1; die namentliche Nennung nachfolgender Überarbeitungen steht noch unter dem Vorbehalt seiner direkten Zustimmung und wird hier nicht geltend gemacht. Die Gutachter früherer Entwürfe des vorangegangenen Implementierungsberichts (v0.4) lieferten einen Rahmen, der in diesen Artikel eingeflossen ist; ihre Beiträge werden dankbar gewürdigt.

Anhang A – Reproduzierbarkeit

Ein Gutachter, der die Reproduzierbarkeit der Architektur überprüfen möchte, kann dies auf den folgenden Ebenen tun.

Das Tractatus-Framework ist die vollständig öffentliche Komponente, die unter `codeberg.org/mysovereignty/tractatus-framework` unter Apache 2.0 bereitgestellt wird. Sein Arbeitspapier dokumentiert die Beobachtungsergebnisse des Frameworks und die darin kodifizierten Architekturmuster. Ein Prüfer mit Zugriff auf eine Installation der Claude-Code-Klasse kann die Musterbibliothek des Frameworks reproduzieren und die Aufzeichnung von Konsultationen in einer lokalen Datenbank nachbilden.

Die veröffentlichten Module der Plattform – unter EUPL-1.2 in der modulweisen Veröffentlichung – bilden die architektonische Oberfläche, die externe Prüfer nutzen können. Die bisherigen Module umfassen das Kern-Plugin „sovereign-record“, die Policy Inheritance Engine, den Tenant-Key-Store, Komponenten der DSR-Pipeline und die Infrastruktur zur Aufzeichnung von Framework-Konsultationen.

Architektonische Komponenten werden in diesem Artikel auf der Ebene ihrer Interaktionen und Verträge beschrieben. Spezifische Quellpfade (Dateinamen innerhalb des Quellbaums der Plattform) werden bewusst nicht aufgeführt; die Reproduzierbarkeit auf Datei- und Zeilenebene wird durch die veröffentlichten Module gewährleistet, während operative Einzelheiten (Bereitstellungspipeline, Wartungsschritte, Hook-Optimierung) als technische Details und nicht als Forschungsbeitrag zurückgehalten werden.

Skripte zur Verifizierung von Anwendungsfällen folgen einer

Namenskonventionvom Typ „validate-use-cases-*"; Skripte zur Aufzeichnung von Framework-Konsultationen folgen einer Namenskonventionvom Typ „record-*-consultation“. Jedes Konsultationsskript erzeugt eine idempotente Einfügung von Datensätzen in lokale sowie EU-souveräne und NZ-souveräne Produktionsdatenbanken unter einer Revisionskennung.

Die Reproduktion des Rahmenkonsultationsmusters aus Sicht des Tractatus-Frameworks ist in [1] dokumentiert.

Anhang B – Momentaufnahme des Use-Case-Verifizierungs-Ledgers

Ein aktueller Snapshot des Anwendungsfall-Ledgers umfasst mehr als 45 unterschiedliche Validierungsskripte. Jedes Skript überprüft eine benannte Eigenschaft einer Architekturkomponente anhand einer aktiven lokalen Datenbank; die Skripte sind unabhängig voneinander und in ihrer Gesamtheit ausführbar. Die folgenden Kategorien fassen den Skriptsatz zusammen; die Anzahl der Szenarien pro Skript sowie die PASS/FAIL-Ergebnisse sind in den internen Artefakten des Projekts enthalten und können von einem externen Prüfer mit Zugriff auf den Code reproduziert werden:

- Kanonisierung der Herkunft und Stabilität über Hydrationsmodi hinweg
- Policy Inheritance Engine: Kernauflösung; Gate-and-Filter-Verkabelung; Origin-Only-Filterung; Filterung im Gruppenbereich; strikter Modus für unbekannten Bereich Verifizierungs-Caching: Erfassungsdienst; Post-Save-Hook + geplanter
- Verifizierungs-Caching: Erfassungsdienst; Post-Save-Hook + geplanter Sweep; Read-Path-Integration; Update-Path-Post-Save-Hook
- Tenant-Schlüsselspeicher: Lebenszyklusoperationen
- Signierung der Beweiskette: CREATE-Consumer; UPDATE/DELETE im Dokumentmodus; DELETE im Abfragemodus; UPDATE im Abfragemodus; Tombstone in der Governance-Warteschlange
- DID-Veröffentlichung: Mandanten- + Mitgliedsdokumente
- Verbindung der Governance-Warteschlange
- Export-Wrapper: modusspezifisches Verhalten; Integration; Erfolgspfad-Auditprotokollierung; Sichtbarkeitsüberlagerung für Hash- und Aggregatmodi
- Verfassungsrechtliche Voraussetzungen und mehrsprachige Unterstützung
- Migration souveräner Datensätze: über die vom Mandanten generierten Top-Level- Modelle hinweg; Abdeckung eingebetteter Unterdokumente (NewsPost, Resource, EventMenu, Edition); Unterdokumente Phasen 1+2
- Verknüpfung auf Gruppenebene und formübergreifende Zuordnung
- DSR-kanonischer Export: Bündelzusammenstellung; Signierung des Manifests; Ehrlichkeit des Trunkierungsflags; End-to-End-Erfassung beim empfangenden Mandanten

- Worker-Policy-Gate: Hilfs-Unit-Tests; Integration pro Worker (EmailProcessor, DocumentScanner)
- WebSocket-Richtlinienadapter
- Nachrüstung von Tombstones
- Verdichtung der Proof-Chain
- Föderationsoberfläche: Negativtestmatrix über zwölf Kategorien, mit einer Teilmenge, die von einem Live-Multi-Tenant-Validator durchlaufen wird

Anhang C – Referenz zum Manifestschema der Föderation

Ein Föderationsvereinbarungsdatensatz enthält das bilaterale Manifest auf Architekturkomponentenebene. Das Schema benennt: die Abkommens-Kennung; jede Partei (Mandanten-Kennung, dezentrale Mandanten-Kennung, Signatur, Zeitstempel der Signatur); den begrenzten Zweck (eine Aufzählung: Fahrgemeinschaftsvermittlung; gemeinsame Veranstaltungsankündigung; gemeinsame Beratung; gemeinsame Verwaltung von Kaupapa; domänenübergreifende Namensreferenz; und andere); die Datenflussform pro Richtung (offengelegte Felder ; angewandte Transformation; Aufbewahrung auf der Empfängerseite); die Regel zur Richtlinienauflösung (welche Verfassung gilt; wie Richtlinienkonflikte gelöst werden, einschließlich einer expliziten Tabelle pro Feld); das Widerrufsverfahren (einseitig durch eine der Parteien; sofortige Weitergabe; beide Parteien behalten eine signierte Kopie zur Nachverfolgung); und die Identifikatoren für die Aufbewahrung von Nachverfolgungsdaten (mandantenübergreifende Abfrageprotokolle auf jeder Seite). Das Manifest selbst enthält den Standard-Metadatenblock für souveräne Datensätze (Herkunft, Richtlinie, Verschlüsselung, Beweiskette, Verifizierungs-Cache); eine Föderation wird nicht aktiviert ohne verifizierte Signaturen beider Parteien gegenüber ihren jeweiligen DID-Dokumenten .

Spezifische Details zu den Feldsätzen der Implementierung, die über diese architektonische Struktur hinausgehen, werden gemäß der IP-Perimeter-Richtlinie (§13.2) zurückgehalten. Gutachter, die vollständige Schemaspezifikationen für die Kompatibilitätsbewertung benötigen, können diese durch direkte Anfrage an den entsprechenden Autor unter Einhaltung angemessener Vertraulichkeit erhalten.

Referenzen

[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). *Verteilungsgerechtigkeit durch Struktur – Ein Anwendungsbeispiel für Wertebeständigkeit auf Gemeindeebene, 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). Die CARE-Prinzipien für die Datenverwaltung indigener Völker . *Data Science Journal*, 19(1), 43. doi.org/10.5334/dsj-2020-043.

[5] Waitangi Tribunal. (2011). *Ko Aotearoa Tēnei: Ein Bericht über Ansprüche bezüglich neuseeländischer Gesetze und Politik, die die Kultur und Identität der Māori betreffen (WAI 262).* Legislation Direct, Wellington.

[6] Europäische Kommission. (2024). *Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Künstliche-Intelligenz-Gesetz).*

[7] Europäische Kommission. (2024). *Verordnung (EU) 2024/1083 des Europäischen Parlaments und des Rates vom 11. April 2024 zur Schaffung eines gemeinsamen Rahmens für Mediendienste im Binnenmarkt (Europäisches Medienfreiheitsgesetz).*

[8] Europäisches Parlament und Rat. (2016). *Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung),* Artikel 9, 15, 16, 17, 18, 20, 21.

[9] US-Kongress. (2018). *Clarifying Lawful Overseas Use of Data Act (CLOUD Act),* Pub. L. Nr. 115–141, Div. V (23. März 2018).

[10] European Union Public Licence v1.2 (EUPL-1.2). https://joinup.ec.europa.eu/collection/eupl. Genehmigt von der Europäischen Kommission, 2017.

[11] World Wide Web Consortium. (2022). *Dezentrale Identifikatoren (DIDs) v1.0 – Kernarchitektur, Datenmodell und Darstellungen.* W3C-Empfehlung.

[12] Stroh, J. G. (2026). *Sovereign-Record-Architektur für Plattforen auf Community-Ebene – Ein Bericht zur Umsetzung der Phase 1, v0.4.* My Digital Sovereignty Limited (NZ). Vorläufiger Entwurf zu diesem Papier; als historischer Nachweis des Architekturzustands in Phase 1 aufbewahrt.

[13] Radio New Zealand / 1News. (Februar 2026). *MFAT bestätigt Gespräche über eine erweiterte Partnerschaft zur Grenzsicherheit mit den Vereinigten Staaten.* Offizielle Stellungnahme des Ministeriums für auswärtige Angelegenheiten und Handel.

[13a] Waitangi Tribunal. *Untersuchung WAI 2522.* Zwei Abschlussberichte, die für dieses Papier relevant sind: (i) *Bericht über das Transpazifische Partnerschaftsabkommen* (2016); (ii) *Bericht über das Umfassende und Fortschrittliche Abkommen zur Transpazifischen Partnerschaft* (2021). Ein dritter Bericht im Rahmen derselben Untersuchung WAI 2522 – *Bericht*

über die Überprüfung des Sortenschutzsystems durch die Krone (2020) – ist thematisch verwandt, wird hier jedoch nicht zitiert. Alle Berichte sind unter waitangitribunal.govt.nz verfügbar.

[14] Centrist.nz. (2026). *Abkommen zwischen Neuseeland und den Vereinigten Staaten zur Grenzsicherheit: Stand der Verhandlungen.* Abgerufen über die Berichterstattung von centrist.nz zu den EBSP-Gesprächen.

[15] Oceanic Press. (2026). *EBSP-Gespräche: Beamte bestätigen Verhandlungsumfang und -anforderungen.*

[16] Privacy Foundation New Zealand. (2026). *Stellungnahme zum Austausch biometrischer Daten mit den Vereinigten Staaten im Rahmen der Enhanced Border Security Partnership.* Medienmitteilung der Privacy Foundation NZ . [17] Biometric Update. (2026). Neuseeland erwägt *im* Rahmen *der* EBSP-Gespräche den Zugang der USA zu biometrischen Daten und Identitätsinformationen von Bürgern.

[17] Biometric Update. (2026). *Neuseeland erwägt im Rahmen der EBSP-Gespräche den Zugang der USA zu biometrischen Daten und Identitätsinformationen seiner Bürger. [18] Gunasekara, G. (2026). Analyse der Enhanced Border* Security Partnership und der Bestimmungen des DHS zum direkten Datenbankzugriff. Rechtskommentar der University of Auckland .

[18] Gunasekara, G. (2026). *Analyse der Enhanced Border Security Partnership und der Bestimmungen des DHS zum direkten Datenbankzugriff.* Rechtskommentar der University of Auckland.

[19] Cochrane, T. (2024). *Sollte Neuseeland ein Abkommen im Stil des CLOUD Act anstreben? Auswirkungen auf den digitalen Datenschutz.* Vom Datenschutzbeauftragten finanzierte Studie.

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

[21] Bluesky Public Benefit Corporation. (2024). *AT-Protokoll- Spezifikation.* https://atproto.com. Account-Portabilität + dezentrale Identifikator- (DID-basierte) Handle-Auflösung.

[22] Mansour, E., Sambra, A. V., Hawke, S., Zereba, M., Capadisli, S., Ghanem, A., Aboulnaga, A., & Berners-Lee, T. (2016). *Eine Demonstration der Solid-Plattform für Social-Web-Anwendungen.* Begleitheft zur 25. Internationalen Konferenz zum World Wide Web. Sowie die laufenden Spezifikationsarbeiten der W3C Solid Community Group unter https://solidproject.org.

[23] McMahan, H. B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017). *Kommunikationseffizientes Lernen von Deep Networks aus dezentralen Daten.* In *Artificial Intelligence and Statistics (AISTATS).* Die ursprüngliche Veröffentlichung zum föderierten Lernen.

[24] Kairouz, P., et al. (2021). *Fortschritte und offene Probleme im föderierten*

Lernen. Foundations and Trends in Machine Learning, 14(1-2), 1-210. Umfassende Übersicht über Architekturentscheidungen und offene Probleme im Bereich des föderierten Lernens.

[25] Walter, M., & Suina, M. (2019). *Indigene Daten, indigene Methodologien und indigene Datenhoheit. International Journal of Social Research Methodology*, 22(3), 233-243.

[25a] Taiuru, K. (3. Mai 2026). *KI-Agenten und Rechtspersönlichkeit in Neuseeland.* `taiuru.co.nz/ai-agents-and-legal-personhood-in-new-zealand/`. Zugriff am 03.05.2026. Meinungsbeitrag (enthält den ausdrücklichen Haftungsausschluss des Autors in persönlicher Eigenschaft). Stellt die Frage der Rechtspersönlichkeit als offene Untersuchung dar und überlässt die Entscheidung der gemeinsamen Arbeit von KI-Entwicklern, Regierungsbehörden und Māori-Gemeinschaften.

[25b] Taiuru, K. (6. März 2026). *Kaupapa Māori AI Framework — He Tangata, He Karetao, He Ātārangi.* `taiuru.co.nz/kaupapa-maori-ai-framework/`. Abgerufen am 04.05.2026. KI-Rahmenwerk für indigene Völker, das auf dem Te Tiriti o Waitangi und der UNDRIP basiert; nennt die Zustimmung der Māori und die Datenhoheit über Trainingsmaterial sowie die lückenlose Rechenschaftspflicht über Entwickler, Betreiber und Anwender hinweg als vorgeschriebene Praxis.

[22b] Symmetry Systems. (2024). *Securing Your Sovereign Data+AI Stack.* Branchenanalyse zur Architektur souveräner KI.

[23b] Merit Data Tech. *Zero-Egress AI: Architektur von lokal installierten Sprachmodellen für überprüfbare Datenhoheit.* Branchenanalyse . [24b] Enterprise DB. Sovereign AI: Gewährleistung von *Daten-* und KI- *Hoheit* in Unternehmen.

[24b] Enterprise DB. *Souveräne KI: Gewährleistung von Daten- und KI-Souveränität in Unternehmen.*

[26] Wachter, S., Mittelstadt, B., & Floridi, L. (2017). *Warum ein Recht auf Erklärung automatisierter Entscheidungsfindung in der Datenschutz-Grundverordnung nicht existiert.* International Data Privacy Law, 7(2), 76–99. DOI: 10.1093/idpl/ipx005. Zitiert in §3.5.

[27] Edwards, L., & Veale, M. (2017). *Sklave des Algorithmus? Warum ein „Recht auf Erklärung“ wahrscheinlich nicht die Lösung ist, nach der Sie suchen.* Duke Law & Technology Review, 16(1), 18–84. Verfügbar unter scholarship.law.duke.edu/dltr/vol16/iss1/2. Zitiert in §3.5.

[28] Te Mana Raraunga (Māori Data Sovereignty Network). (2018, Oktober). *Principles of Māori Data Sovereignty.* Abgerufen unter temanararaunga.maori.nz/principles-of-maori-data-sovereignty. Zitiert 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. Zitiert in §3.6.

[30] Hudson, M., Anderson, T., Dewes, T. K., Temara, P., Whaanga, H., & Roa, T. (2017). *„He Matapihi ki te Mana Raraunga“ — Konzeptualisierung von Big Data aus der Perspektive der Māori.* Verfügbar über Research Commons, University of Waikato. Zitiert in §3.6.

[31] Raman, A., Joglekar, S., De Cristofaro, E., Sastry, N., & Tyson, G. (2019). *Herausforderungen im dezentralen Web: Der Fall Mastodon.* In: Proceedings of the Internet Measurement Conference 2019 (IMC '19), Amsterdam, Oktober 2019. Empirische Charakterisierung des Mastodon-Föderationsgraphen, der Instanzkonzentration und der operativen Anfälligkeit unter Moderation auf Instanzebene.

[32] Zignani, M., Gaito, S., & Rossi, G. P. (2018). *Follow the „Mastodon“: Struktur und Entwicklung eines dezentralen sozialen Online-Netzwerks.* In: Proceedings of the Twelfth International AAAI Conference on Web and Social Media (ICWSM 2018), Stanford, Juni 2018. Strukturanalyse des frühen Mastodon-Netzwerks, einschließlich Clusterbildung auf Instanzebene und Eigenschaften des Föderationsgraphen.

[33] Open Data Institute. (Oktober 2018). *Definition eines „Data Trust“.* ODI-Arbeitspapier. Legt die Arbeitsdefinition eines Data Trust als „eine Rechtsstruktur, die eine unabhängige Verwaltung von Daten gewährleistet“ fest, die in der nachfolgenden Literatur der britischen Regierung und Politik zur institutionellen Gestaltung der Datenverwaltung verwendet wird.

[34] Element AI / Nesta. (2019). *Data Trusts: Ein neues Instrument für die Daten- Governance.* Gemeinsam veröffentlichte Forschungsarbeit zur institutionellen Gestaltung von Data Trusts als Mechanismus zur Bewältigung von Machtungleichgewichten zwischen Technologieunternehmen, Regierung und Öffentlichkeit.

Korrespondenzautor: John G. Stroh, Direktor, My Digital Sovereignty Limited (NZ). ORCID: 0009-0005-2933-7170. E-Mail: john.stroh@mysovereignty.digital.

Vorgeschlagene Zitierweise (nach Genehmigung durch den Betreiber): Stroh, J. G. (2026). *Sovereign-Record-Architektur für Plattformen auf Community-Ebene — Paper A.* My Digital Sovereignty Limited. (Zenodo-DOI wird bei Veröffentlichung zugewiesen.)

Entwurfsstatus: Überarbeitungsentwurf v4 – Mai 2026. Kommentare und Korrekturen sind willkommen. Basiert auf dem vorherigen Implementierungsbericht v0.4. Die Struktur umfasst „Related Work“, „Threat Model“ und „Evaluation“ gemäß Schritt C des Neupositionierungsplans vom 01.05.2026. Begleitartikel (Artikel B – Situated Language Layers, Zusammenfassung der Die Struktur

umfasst nun „Related Work“, „Threat Model“ und „Evaluation“ gemäß Schritt C des Neupositionierungsplans vom 01.05.2026. Begleitpapier (Paper B – Situated Language Layers, Zusammenfassung des empirischen Begleitpapiers, veröffentlicht). Veröffentlicht unter agenticgovernance.digital als Überarbeitungsentwurf; Zenodo-DOI wird in der Release-Candidate-Phase von v4 zugewiesen.