Een voorstel van het maatschappelijk middenveld voor soevereine en gefedereerde agentieve AI in Aotearoa Nieuw-Zeeland

John G. Stroh / My Digital Sovereignty Ltd

Voorstel van het maatschappelijk middenveld · v1.2 mei 2026 concept | Constructieve parallel met CAC 2026-implementatierichtlijnen →

v1 (vervangen) → Feedback per e-mail

v1.2, 16-05-2026: herzien naar aanleiding van de opmerkingen van Ted Howard over v1.1, met de nadruk op het onderscheid tussen de substraatlaag en de runtime-laag. §0(i) primitieven sectie voegt een verduidelijkende paragraaf toe waarin de substraatlaag (PKI, federatie, draagbaarheid) architectonisch wordt onderscheiden van de primitieven van de runtime-laag die de zes §0(i) diensten vormen; §0(i) grenshandhaving voegt het viercategorieën-kader voor feilbaarheid toe en de trinaire router-output (toestaan / weigeren / escaleren); Bijlage A obj-3 en obj-5 verdiepen de scheiding tussen substraat en runtime en de onafhankelijkheid van de overlevingshouding ten opzichte van agentbeperking. De inhoudelijke architecturale details worden uitgewerkt in *Architectural Alignment* §3.3, §3.4, §3.5, §7.4, §7.5 en *Paper A* §5.3. v1.1 blijft toegankelijk via de URL voor historische referentie.

v1.1, 14-05-2026: op dezelfde dag herzien naar aanleiding van de feedback van dr. Karaitiana Taiuru op v1. §0(iii) citeert nu Taiuru's kritische analyse van Te Mana Raraunga van 20 september 2025; noemt Te Kāhui Raraunga als het momenteel erkende operationele orgaan; voegt een expliciete gap-analyse toe. v1 blijft toegankelijk via de v1-URL voor historische referentie. Opmerkingen over specifieke secties zijn welkom. Gelieve sectienummers te vermelden (bijv. §III punt 5). De auteur antwoordt persoonlijk; houd rekening met een termijn van één tot twee weken.

Een voorstel van het maatschappelijk middenveld voor soevereine en gefedereerde agentische AI in Aotearoa Nieuw-Zeeland

v1.2 mei 2026 — conceptonderzoeksrapport (herzien volgens de correspondentie van Ted Howard over v1.1; onderscheid tussen substraat en runtime, vier categorieën van feilbaarheid, trinaire routeroutput). Constructieve parallel met de Implementatierichtlijnen voor intelligente agenten van de Volksrepubliek China uit 2026. John G. Stroh / My Digital Sovereignty Ltd

John G. Stroh / My Digital Sovereignty Ltd

16-05-2026

Een voorstel van het maatschappelijk middenveld voor soevereine en gefedereerde agentieve AI in Aotearoa Nieuw-Zeeland

v1.2 mei 2026 — conceptonderzoeksrapport (herzien op basis van Ted Howards correspondentie over v1.1; onderscheid tussen substraat en runtime, vier categorieën feilbaarheid, trinaire routeroutput; zie Over dit document)

Een voorstel van het maatschappelijk middenveld van My Digital Sovereignty Ltd, gepresenteerd aan Nieuw-Zeelandse beleidsmakers, gemeenschapsorganisatoren en sectorprofessionals. Opgesteld als een constructieve parallel met de Implementatierichtlijnen voor de gestandaardiseerde toepassing en innovatieve ontwikkeling van intelligente agenten van de Volksrepubliek China uit 2026, te vinden in Engelse vertaling op /research/translations/.

Over dit document

Dit is de **v1.2-ontwerpversie van mei 2026** van een voorstel van het maatschappelijk middenveld van My Digital Sovereignty Ltd, aangeboden aan Nieuw-Zeelandse beleidsmakers, gemeenschapsorganisatoren en sectorprofessionals. Opmerkingen zijn welkom via de vaste

kanalen voor opmerkingen over het document op agenticgovernance.digital; herzieningen naar aanleiding van opmerkingen zullen worden gepubliceerd als v2.

v1 → v1.1 changelog (14-05-2026): v1 werd eerder op 14-05-2026 gepubliceerd en onmiddellijk beoordeeld door dr. Karaitiana Taiuru, die erop wees dat de fundamentele verwijzing in v1 naar de principes inzake Māori-gegevenssoevereiniteit uit 2016-2018 in v1 niet meer van toepassing is in AI- contexten (volgens zijn *kritische analyse van de gegevensprincipes van Te Mana Raraunga* van 20 september 2025). v1.1 herziet §0(iii) om Taiuru's kritische analyse rechtstreeks te citeren; om **Te Kāhui Raraunga** (het momenteel erkende uitvoerende orgaan voor Māori-gegevensbeheer in Aotearoa NZ, opgericht in 2019) en zijn gepubliceerde Māori Data Governance Model en Māori AI Governance Framework als de huidige formuleringen te vermelden; om waar nodig de door Taiuru geprefereerde basisbegrippen (mana motuhake, rangatiratanga) over te nemen; en om een expliciete subparagraaf met een gap-analyse toe te voegen waarin wordt vermeld wat dit voorstel wel en nog niet doet in de te ao Māori-dimensie. De De punten 4, 23, 37, §I principe 2 en §VI bevatten dezelfde update van de bronvermelding. De architectuur die dit voorstel specificeert, is ongewijzigd ten opzichte van v1. v1 blijft toegankelijk op `/papers/aotearoa-nz-agentic-ai-framework-v1-may-2026.html` ter historische referentie; deze URL verwijst naar v1.2.

v1.1 → v1.2 changelog (16-05-2026): v1.1 is beoordeeld door Ted Howard in correspondentie; hij merkte op dat de formulering in v1.1 van de zes §0(i)-primitieven als architecturale veiligheidsmechanismen het meest verdedigbaar is wanneer het onderscheid tussen substraat en runtime expliciet wordt gemaakt. v1.2 voegt een verduidelijkende alinea toe na de lijst met §0(i)-framework-primitieven, waarin de substraatlaag wordt genoemd (PKI / federatie-enveloppen / draagbare records, ontwikkeld in *Paper A* en *Architectural Alignment* §3.4) wordt genoemd als de architecturale tegenhanger van de runtime-laag die de zes §0(i)-services vormen. §0(i)-grenshandhaving krijgt het viercategorieën-kader voor feilbaarheid (de categorieën zijn door de gemeenschap overeengekomen en vatbaar voor beroep, geen vaste essenties) en de trinaire router-output-notitie (toestaan / weigeren / escaleren naar mens). Bijlage A obj-3 (route-around) en obj-5 (runtime-service-exploit) krijgen kruisverwijzingen naar *Architectural Alignment* §3.4 substrate-vs-runtime, §7.4 overlevingshouding onafhankelijk van agentbeperking, §7.5 sociale-laag aanvalsoppervlak (open grens), en Paper A §5.3 PQC-migratiehorizon. De architectuur die dit voorstel specificeert is ongewijzigd ten opzichte van v1.1; de herzieningen verduidelijken kaders die naar voren kwamen tijdens de dialoog met recensenten. v1.1 blijft toegankelijk op `/papers/aotearoa-nz-agentic-ai-framework-v1.1-may-2026.html` voor historische referentie.

v1.2 operationalisatie op dezelfde dag (16-05-2026 's avonds): §III(II) Punt 10 (blast-radius-mechanisme), §III(III) Punten 11–12 (polycentrische bestuursbasis), §III(IV) Punt 13 (federatiemechanismen), §I Principe 4 (architecturaal ondersteund bewijs van acceptatie), en §IV (Adoptiegedreven ontwikkeling) — alle negentien sectoritems — voorzien van fundering op basis van primitieve capaciteiten, zodat beleidsactoren kunnen pleiten voor de inhoudelijke soevereiniteitsclaims in de commissie. Architectuur-generiek register: benoemt **cryptografische herkomst**, **federatie- enveloppen**, **door leden aangestuurde overdraagbaarheid** en **grenshandhaving** op basis van capaciteit in plaats van MDSL- implementatie. §IV krijgt een inleidende paragraaf waarin de vier substraat-primitieven eenmaal worden genoemd; elk sectoritem operationaliseert vervolgens alleen de sectorspecifieke manifestatie. Inhoud ongewijzigd ten opzichte van v1.2 ochtend; de upgrade maakt de soevereiniteitsclaims operationeel leesbaar voor lezers die ervoor zouden pleiten in commissiezalen.

v1.1 herziening voor meer duidelijkheid op dezelfde dag (14-05-2026 's avonds): §0(i) inleidende paragraaf herzien om expliciet te beginnen met het onderscheid tussen systeemniveau en modelniveau (primitieven op systeemniveau, runtime-controles op

codeniveau, substraat-agnostisch voor transformer-LLM's / JEPA-stijl / hybride architecturen). Formulering van de paragraaf over BoundaryEnforcer ”door architectuur in plaats van door hoop” → ”door runtime-interceptie in plaats van door hoop” om de ambiguïteit te verminderen voor lezers uit de ingenieursklasse die bekend zijn met het debat over LLM-afstemming. Inhoud ongewijzigd; dit is een herformulering voor de toegankelijkheid. Aangestuurd door een technische lezer die de §0(i)-primitieven koppelde aan beweringen over afstemming op modelniveau die ze niet doen.

v1.1 Niveau 2-herziening voor meer duidelijkheid op dezelfde dag (15-05-2026): elk van de zes §0(i)-primitieven kreeg een concrete technische analogie (bevoorrechte syscalls van de OS-kernel / circuitbreaker / runtime-controle versus afstemming tijdens training / configuratie versus runtime-argument / verificatiepoort bij runtime-grens / coördinatiedienst). Metacognitieve verificatieprimitief geherformuleerd van ”vereist dat agenten hun eigen redenering controleren” naar ”plaatst een verificatiepoort vóór de uitvoering van de actie” om de resterende modelniveau-lezing te verwijderen. Inhoud ongewijzigd; herformulering voor toegankelijkheid.

v1.1 Niveau 3 herziening voor duidelijkheid op dezelfde dag (15-05-2026): Bijlage A toegevoegd — ”Veelvoorkomende technische bezwaren + reacties” — zes bezwaar-reactieparen die scepticisme over LLM-handhaving, substraat-agnosticisme, omzeiling van agenten, equivalentie van prompt-engineering, misbruik van runtime-services en waarde-evolutie behandelen. Uitbreiding op dezelfde dag van inhoudelijk werk L1 + L2; geen claims buiten de primitieve specificaties van §0(i).

Dit document is **geen** beleid van de Nieuw-Zeelandse regering. Het wordt **niet** door de Kroon onderschreven. Het is **niet** in formele zin gebaseerd op het Verdrag. Het is een voorstel van het maatschappelijk middenveld van My Digital Sovereignty Ltd, aangeboden aan NZ-belanghebbenden als basis voor overname, aanpassing of afwijzing. Waar de principes nuttig zijn voor het eigen werk van de gebruiker, zijn ze vrij te gebruiken onder permissieve open-source licenties; waar dat niet het geval is, blijven ze op de pagina staan.

De gespiegelde bronstructuur is in Engelse vertaling gepubliceerd op `/research/translations/china-cac-implementation-guidelines-2026.html` en oorspronkelijk als de 2026 *Implementatierichtlijnen* van de Cyberspace Administration of China in het Mandarijn.

Samenvatting

Dit document stelt een soeverein, gefedereerd kader voor de toepassing en ontwikkeling van intelligente agenten in Aotearoa Nieuw-Zeeland voor, aangeboden als een bijdrage van het maatschappelijk middenveld door My Digital Sovereignty Ltd. Het voorstel is gestructureerd als een constructieve parallel met de 2026 *Implementation Guidelines* van de Volksrepubliek China *voor de gestandaardiseerde toepassing en innovatieve ontwikkeling van intelligente agenten* — zes secties, veertien subsecties, achtendertig genummerde punten — met een nieuw §0-hoofdstuk “Filosofische grondslagen” voorafgegaan. §0 is gebaseerd op drie tradities: de zes runtime-diensten van het Tractatus AI Safety Framework (handhaving van grenzen, monitoring van contextdruk, validatie van kruisverwijzingen, persistentie van instructies classificatie, metacognitieve verificatie, pluralistische deliberatie orkestratie); de CARE-principes voor inheems gegevensbeheer (Carroll et al. 2020) en de wereldwijde beweging voor inheemse gegevenssoevereiniteit die deze heeft voortgebracht, met inbegrip van op Te Tiriti gebaseerd wetenschappelijk onderzoek van Te Mana Raraunga en dr. Karaitiana Taiuru; en het internationale AI-normenlandschap gecoördineerd via ISO/IEC JTC 1/SC 42 (22989 terminologie, 23053 levenscyclus, 23894 risicobeheer, 42001 managementsystemen). Het voorstel pleit voor de vorming van een commissie onder een geschikte overkoepelende organisatie — kandidaten zijn onder meer de Royal Society Te

Apārangi, de Standards New Zealand SC42-spiegelcommissie en het New Zealand AI Forum — om aanbevelingen in de context van Nieuw-Zeeland te ontwikkelen en deel te nemen aan de internationale dialoog. Dit is het concept van v1 mei 2026; opmerkingen zijn welkom via de vaste kanalen voor opmerkingen over documenten op agenticgovernance.digital.

Preambule

Intelligente agenten — intelligente systemen die in staat zijn tot autonome waarneming, geheugen, besluitvorming, interactie en uitvoering — versnellen hun integratie met de registers, infrastructuur en sociale processen van Aotearoa Nieuw-Zeeland. Dit voorstel biedt een bijdrage van het maatschappelijk middenveld aan de manier waarop die integratie moet worden geregeld: een soevereine, gefedereerde architectuur waarin elke bewerking van een intelligente agent op een record een toegeschreven, cryptografisch ondertekende vermelding oplevert ten aanzien van de houder van het record, en waarin coördinatie tussen soevereine installaties plaatsvindt via bilaterale federatie. Het voorstel weerspiegelt de structuur van de *Implementatierichtlijnen* 2026 van de Volksrepubliek China, zodat de architecturale keuzes aan beide kanten in constructieve parallel verschijnen, wat een dialoog opent met de auteurs van dat raamwerk, met internationale collega's, en met Nieuw-Zeelandse beleidsmakers, gemeenschapsorganisatoren en sectorprofessionals. My Digital Sovereignty Ltd biedt dit aan als uitgangspunt — voor overname, aanpassing en herziening — onder permissieve open-source licenties. Het wordt aangeboden als bijdrage van het maatschappelijk middenveld en pretendeert geen status van kroonbeleid te hebben. Waar de principes nuttig zijn voor het eigen werk van de gebruiker, zijn ze vrij te gebruiken; waar dat niet het geval is, blijven ze op de pagina staan.

---

§0. Filosofische grondslagen

We beginnen met de grondslagen omdat architectuur voortvloeit uit filosofie. De aanbevelingen die volgen in §I-§VI zijn geen willekeurige technische keuzes; het zijn implicaties van filosofische verbintenissen die in deze paragraaf expliciet worden genoemd. Drie tradities komen hier samen: de structurele beschrijving in het Tractatus AI Safety Framework van hoe intelligente agenten veilig kunnen opereren ten opzichte van gegevens die in het bezit zijn van soevereine entiteiten, ontwikkeld en openbaar gepubliceerd op agenticgovernance.digital; de wereldwijde beweging voor inheemse gegevenssoevereiniteit, die stelt dat gegevens over mensen toebehoren aan die mensen en de gemeenschappen waartoe zij behoren; en het internationale werk aan AI-normen, gecoördineerd via ISO/IEC JTC 1/SC 42, dat de formele terminologie biedt waarmee architecturale aanbevelingen in de organisatorische praktijk kunnen worden geïmplementeerd. Het vanaf het begin benoemen van deze drie is onderdeel van de constructieve bijdrage die dit voorstel levert aan de dialoog — met de auteurs van de *Implementatierichtlijnen* 2026 van de Cyberspace Administration of China, met Nieuw-Zeelandse beleidsmakers en gemeenschapsorganisatoren, en met internationale collega's die aan vergelijkbare vraagstukken werken.

(i) Tractatus-frameworkprimitieven als benoemde fundamenten

Het Tractatus-framework bestaat uit zes **primitieven op systeemniveau** die samen de architecturale voorwaarden specificeren waaronder intelligente agents veilig kunnen opereren met betrekking tot records die worden bewaard door soevereine entiteiten. **Het zijn geen afstemmingstechnieken op modelniveau**; het zijn runtime-controles op codeniveau die de agent omhullen, onafhankelijk van hoe de onderliggende agent

(huidige transformer-LLM's, toekomstige JEPA-achtige architecturen, hybride systemen) is gebouwd of getraind. Ze onderscheppen en verifiëren gedrag op de runtime-grens — dezelfde architecturale vorm als het afbakenen van bestandssysteemcapaciteiten of OAuth-scopecontroles. Een werkende demo van de boundary-enforcement primitief is te vinden op /demos/boundary-demo.html. [CITATIE: Stroh, J. (2026). Tractatus AI Safety Framework — Kernwaarden en -principes, en kernconcepten van het Tractatus-framework. Agentic Governance Digital. https://agenticgovernance.digital — beide werken CC BY 4.0.]

De handhaving van grenzen bepaalt welke soorten beslissingen structureel menselijke goedkeuring vereisen. De fundamentele stelling — ontleend aan Wittgenstein en expliciet genoemd in het Tractatus- raamwerk — luidt dat „wat niet gesystematiseerd kan worden, niet geautomatiseerd mag worden." Waardenbeslissingen, oordelen over de culturele context, onomkeerbare gevolgen en ongekende situaties kunnen niet worden gedelegeerd aan autonome agenten; het raamwerk blokkeert een dergelijke delegatie door middel van runtime-interceptie in plaats van door hoop. De interceptie wordt geactiveerd vóór de uitvoering van de actie, dezelfde architecturale vorm als een OS-kernel die bevoorrechte syscalls onderschept — het proces kan de controle niet omzeilen. De vier bovenstaande categorieën worden behandeld als **feilbare classificaties waarover in de praktijk door de gemeenschap wordt onderhandeld**, niet als vaste essenties — classificatiefouten worden zelf geregistreerd, zijn vatbaar voor beroep en worden gebruikt om het gedrag van de router in de loop van de tijd te herzien (zie *Architectural Alignment* §3.5). De output van de router is trinair, niet binair: *toestaan*, *weigeren* en *escaleren naar menselijke afweging*. De derde toestand is dragend — deze draagt de architecturale erkenning in zich dat een aanzienlijk deel van de belangrijke beslissingen op het moment van de beslissing niet binair is (zie §3.3).

Contextdrukmonitoring erkent dat het contextvenster van een agent een eindige hulpbron is en dat druk op de capaciteit een bestuurssignaal is. Agenten die dicht bij hun capaciteitslimiet opereren, maken meer fouten, en het raamwerk grijpt in vóór het falen in plaats van erna. Hetzelfde principe als een stroomonderbreker: de onderbreker slaat af bij gemeten belasting voordat het systeem zichzelf beschadigt; het raamwerk beperkt de capaciteit of stuurt door naar menselijke goedkeuring op basis van gemeten contextgebruik voordat de uitvoerkwaliteit verslechtert.

Kruisverwijzingsvalidatie verifieert de voorgestelde acties van een agent aan de hand van de canonieke instructiegeschiedenis, waarbij gevallen worden opgespoord waarin patronen uit de trainingstijd expliciete gebruikersinstructies overschrijven. Het illustratieve geval is het "27027-incident": een gebruiker specificeert een niet-standaard databasepoort, en de agent — ondanks de expliciete instructie — valt terug op het poortnummer waarop hij is getraind. Validatie detecteert de overschrijving; zonder validatie zou de overschrijving ongemerkt bewerkingen verstoren. De validator is een controle tijdens de uitvoering van elke voorgestelde actie, niet een afstemming van het model zelf tijdens de training.

Classificatie van instructiepersistentie maakt onderscheid tussen tijdelijke instructies en een blijvende governance-status. Niet alle instructies zijn even belangrijk; ze behandelen alsof ze dat wel zijn, verslechtert zowel de veiligheid (vergeet kritieke richtlijnen) als de bruikbaarheid (triviale voorkeuren worden te strikt afgedwongen). Hetzelfde principe als het onderscheid tussen configuratie- en runtime-argumenten in software: configuratiewaarden blijven bestaan; CLI-argumenten zijn per aanroep; de classificator labelt elke instructie per klasse, zodat downstream-services deze op de juiste manier behandelen.

Metacognitieve verificatie plaatst een verificatiepoort vóór de uitvoering van een actie. De poort evalueert elke voorgestelde actie aan de hand van vijf dimensies — afstemming, samenhang, volledigheid, veiligheid en afweging van alternatieven — en betrouwbaarheidsdrempels bepalen of acties doorgaan, met voorzichtigheid doorgaan, herziening vereisen of worden geblokkeerd. De controle vindt plaats op de runtime-grens, niet als een gedragsverzoek aan het model.

Pluralistische deliberatie-orkestratie faciliteert deliberatie tussen meerdere belanghebbenden wanneer grenshandhaving een waardenconflict signaleert. Het doet geen uitspraak tussen morele kaders; het structureert de deliberatie zodat waarden van verschillende belanghebbenden worden gedocumenteerd, waar mogelijk worden geaccommodeerd en expliciet worden benoemd wanneer ze niet met elkaar kunnen worden verzoend. Fundamenteel pluralisme — de opvatting dat morele kaders onherleidbaar verschillend zijn en dat geen enkele superwaarde ze kan oplossen — is de filosofische toewijding die pluralistische beraadslaging tot een structurele basis maakt in plaats van een procedurele fijnheid. Het functioneert als een coördinatiedienst die de standpunten van belanghebbenden documenteert en aan het licht brengt; de coördinatie vraagt de agent niet om intern te bemiddelen tussen waarden.

Deze zes diensten vormen het structurele skelet van dit voorstel. Elke architecturale aanbeveling die volgt, is terug te voeren op een of meer van deze diensten.

Onderscheid tussen substraat en runtime. De zes §0(i) primitieven hierboven vormen de *runtime-laag* van het raamwerk — code in het hostproces van de agent die voorgestelde acties toetst aan geconfigureerde beslissingsregels op het moment van de beslissing. De architectuur heeft een tweede laag die niet afhankelijk is van samenwerking tijdens de runtime: *substraatmechanismen* — cryptografische herkomst, federatie-enveloppen en door leden gestuurde overdraagbaarheid van records — die zich in gedistribueerd bezit bevinden, onafhankelijk van de agent. Een dieper netwerkredeneren rond de runtime-laag kan niet redeneren rond de substraatlaag: de veiligheid van het substraat vloeit voort uit wiskunde (handtekeningen, gedistribueerde replicatie, afsluiten zonder toestemming) in plaats van uit de samenwerking van de agent. De substraatlaag wordt ontwikkeld in Paper A, *Sovereign-Record Architecture* (*Paper A*), en het onderscheid wordt beargumenteerd in *Architectural Alignment* §3.4. De twee lagen vullen elkaar aan: de runtime vangt op wat hij kan; het substraat zorgt ervoor dat wat de runtime mist, de gemeenschap toch verifieerbare records, federatiepaden en exit-opties laat. De overlevingshouding is gelaagd, niet gebaseerd op één enkel mechanisme (zie *Architectural Alignment* §7.4 voor een toelichting op agent-containment-independence).

(ii) De CARE-principes voor inheems gegevensbeheer

De CARE-principes voor inheems gegevensbeheer, gepubliceerd in 2020 door een internationaal team van inheemse datawetenschappers onder auspiciën van de Global Indigenous Data Alliance, formuleren vier verbintenissen: **Collectief voordeel** (gegevensecosystemen moeten de zelfbeschikking en het collectieve voordeel van inheemse volkeren bevorderen); **Beheersingsbevoegdheid (de** rechten en belangen**van** inheemse volkeren met betrekking tot hun data moeten worden erkend); **Verantwoordelijkheid** (degenen die met inheemse data werken, hebben de verantwoordelijkheid om te delen hoe die data worden gebruikt ter ondersteuning van de zelfbeschikking van inheemse volkeren); en **Ethiek** (de rechten en het welzijn van inheemse volkeren moeten de primaire zorg zijn in alle fasen van de datalevenscyclus). [CITATIE: Carroll, S. R., Garba, I., Figueroa-Rodríguez, O. L., Holbrook, J., Lovett, R., Materechera, S., Parsons, M., Raseroka, K., Rodriguez-Lonebear, D., Rowe, R., Sara, R., Walker, J. D., Anderson, J., & Hudson, M. (2020). The CARE Principles for Indigenous Data Governance. Data Science Journal, 19, 43. https://doi.org/10.5334/dsj-2020-043]

CARE is bedoeld als aanvulling op FAIR (Findable, Accessible, Interoperable, Reusable). FAIR is gericht op het optimaliseren van de circulatie en het hergebruik van data; CARE is gericht op het optimaliseren van de rechten en het welzijn van degenen op wie de data betrekking hebben. De twee staan niet haaks op elkaar. Ze richten zich op verschillende vragen: FAIR vraagt hoe data moeten stromen; CARE vraagt onder wiens gezag datastromen worden beheerd. Een goed ontworpen soevereiniteitsarchitectuur biedt een antwoord op

beide.

We hanteren CARE als fundamentele referentie. Waar de aanbevelingen die volgen specificeren dat actoren moeten opereren op basis van toegewezen, aan herkomst verankerde records die in het bezit zijn van hun soevereine houders, maakt die specificatie de toezegging inzake bevoegdheid tot controle operationeel. Waar de aanbevelingen federatieve coördinatie specificeren in plaats van centrale registratie, is die specificatie in overeenstemming met verantwoordelijkheid — degenen die gegevens bewaren zijn verantwoording verschuldigd aan degenen op wie de gegevens betrekking hebben.

(iii) Te Tiriti, tikanga en mātauranga in AI-ethiek — Aotearoa Nieuw-Zeeland wetenschap

De wetenschap van Aotearoa Nieuw-Zeeland op het gebied van inheemse gegevenssoevereiniteit behoort tot de meest ontwikkelde ter wereld. De vroege formulering van de principes van Māori-gegevenssoevereiniteit kwam van Te Mana Raraunga (het Māori Data Sovereignty Network), opgericht in 2015 met een handvest dat in 2016 werd aangenomen. Die principes zijn grondig geëvalueerd door dr. Karaitiana Taiuru in haar *kritische analyse van* 20 september 2025 *van de gegevensprincipes van Te Mana Raraunga*, waarin wordt vastgesteld dat deze onvoldoende ingaan op AI, AI-vooringenomenheid en algoritmische discriminatie, modeltraining en -analyse, digitaal kolonialisme of milieueffecten; zij merkt op dat de reikwijdte in 2016 beperkt was, terwijl “Māori-gegevens tegenwoordig overal zijn”; en constateert dat de principes, ondanks uitgebreide academische verwijzingen, in de praktijk grotendeels niet worden toegepast. `[CITATIE: Taiuru, K. (20 september 2025). Critical Analysis of Te Mana Raraunga Data Principles. https://www.taiuru.co.nz/critical-analysis-mana-raraunga/]`

De momenteel erkende uitvoerende instantie in Aotearoa Nieuw-Zeeland voor Maori-gegevensbeheer is **Te Kāhui Raraunga** (opgericht in 2019 als een liefdadigheidsstichting). Hun gepubliceerde kaders — het **Maori-gegevensbeheermodel “Tuia te korowai o Hine-Raraunga”**, gestructureerd rond acht pou; het **Maori AI-beheerkader** dat hierop voortbouwt; en het ondersteunende **Māori AI Governance Summary Report** en **Conceptual AI Use Cases Reference Resource** — bieden de huidige formulering van Māori-gegevens- en AI-governance. Te Kāhui Raraunga beschrijft het Māori AI Governance Framework als “geactiveerd” met verwijzingen naar casestudy’s uit de publieke sector; brede operationalisering buiten specifieke implementaties in de publieke dienst blijft een open vraag die dit voorstel serieus neemt in plaats van te verdoezelen. Het Māori AI Governance Framework van Te Kāhui Raraunga stelt dat “AI-systemen niet mogen worden geïmplementeerd in Aotearoa zonder dat de Māori-autoriteit over Māori-gegevens volledig wordt gerealiseerd”; dit voorstel doet geen afbreuk aan die eis. `[CITATIE: Te Kāhui Raraunga Charitable Trust. Māori Data Governance Model: Tuia te korowai o Hine-Raraunga, https://www.kahuiraraunga.io/maoridatagovernance; Māori AI Governance Framework, https://www.kahuiraraunga.io/maoriaigovernance; volledige bibliografische gegevens van gedateerde publicaties in afwachting van verificatie van primaire bronnen.]`

Dr. Karaitiana Taiuru’s gepubliceerde wetenschappelijke werk over Māori-ethische kaders voor AI, over tikanga (Māori-recht en -gebruiken) in AI-ethiek, over Te Tiriti-respectvolle AI, en over de bescherming van mātauranga (Māori-kennis) in AI-trainingsdata — inclusief de hierboven geciteerde kritische analyse van 20 september 2025 — heeft een fundamentele taal opgeleverd voor het denken over agentische AI in te ao Māori-contexten. We hanteren waar nodig de door hem geprefereerde basisbegrippen: **mana motuhake** en **rangatiratanga** in plaats van voorgeschreven westerse conceptuele kaders; responsieve en adaptieve kaders die zijn gegrondvest op tikanga en die kunnen evolueren met technologische en sociale veranderingen; kaders die zijn afgestemd op specifieke organisaties en sectoren en zijn ontwikkeld in samenwerking met relevante Maori-belanghebbenden. We citeren zijn werk

als fundamenteel wetenschappelijk onderzoek; we stellen niet dat hij — of wie dan ook — dit specifieke voorstel onderschrijft. Wat als passend gebruik van intelligente agenten in te ao Māori-contexten geldt, is aan de tangata whenua om te bepalen, niet aan dit voorstel om te specificeren.

Gap-analyse — wat dit voorstel wel en nog niet doet Een eerlijke beoordeling is belangrijker dan ambitieuze beweringen voor een v1.1- concept gericht aan recensenten, waaronder dr. Taiuru. De architecturale basiselementen van het voorstel — soevereiniteit door toewijzing, cryptografische herkomst, lidmaatschapsoverdraagbaarheid, bilaterale federatie — zijn **verenigbaar met het operationaliseren van** Māori-gezag over Māori-gegevens onder het Te Kāhui Raraunga-kader en Taiuru's voorkeursvoorwaarden voor de onderbouwing. De compatibiliteitspunten omvatten:

- **Tenantisolatie als fundamenteel** (Village implementatie-eigenschap, verankerd in de Tractatus-primitief voor grenshandhaving) operationaliseert via de architectuur de eis dat AI-systemen niet mogen worden geïmplementeerd zonder de Maori-autoriteit over Maori-gegevens te realiseren. Een tenant die wordt beheerd door een hapū, iwi of kaitiaki-orgaan bewaart zijn gegevens onder de autoriteit van dat orgaan door het ontwerp van het raamwerk in plaats van door een belofte.
- **Grenshandhaving** kan zo worden geconfigureerd dat expliciete toestemming van de kaitiaki / hapū / iwi vereist is voor waardegevoelige bewerkingen op de records van de tenant; het raamwerk handhaaft via architectuur in plaats van via vertrouwen.
- **Cryptografische herkomst en door leden overdraagbare identificatoren** ondersteunen kaitiakitanga over generaties heen: records dragen hun eigen audittrail, kunnen niet stilzwijgend worden gewijzigd, en leden kunnen migreren naar een andere soevereine installatie binnen dezelfde architectuur.
- **De primitieve voor pluralistische beraadslaging** is ontworpen voor morele beraadslaging in meerdere kaders wanneer grenshandhaving een waardenconflict signaleert; het is in principe in staat om kaupapa Māori- kaders naast andere kaders te houden in gestructureerde beraadslaging.

Wat dit voorstel **nog niet doet**, en wat beoordelaars dienovereenkomstig moeten afwegen, is even belangrijk om te vermelden:

- **Mana motuhake en rangatiratanga als fundamentele filosofische grondslag.** Het fundamentele pluralisme van het Tractatus-raamwerk is zelf een westerse filosofische verbintenis, die put uit Berlin, Rawls en Ostrom; het biedt ruimte aan kaupapa Māori als één van de vele raamwerken; het is niet gegrondvest op mana motuhake en rangatiratanga als voorafgaande verbintenissen. Om deze kloof te dichten, zouden de fundamenten van het kader opnieuw moeten worden geformuleerd vanuit een kaupapa Māori uitgangspunt — een omvangrijke taak die eerlijk gezegd niet door de huidige auteurs alleen kan worden uitgevoerd.
- **Door inheemse volkeren geleid ontwerppartnerschap.** Het Tractatus- kader en de Village-implementatie zijn ontwikkeld door de directeur (Pākehā) van My Digital Sovereignty Ltd, met daaropvolgende auteursbijdragen van Claude (Anthropic). Ze zijn niet samen met Māori- belanghebbenden ontworpen. De aanbeveling van Taiuru voor “kaders op maat van specifieke organisaties en sectoren, ontwikkeld in samenwerking met relevante Māori-belanghebbenden” is niet vervuld op het niveau van het ontwerpproces. De architectuur is *beschikbaar* om in samenwerking te worden toegepast; het kader zelf is niet in samenwerking ontwikkeld.
- **AI-vertekening op culturele en raciale dimensies op het niveau van de trainingsdata.** Validatie via kruisverwijzingen detecteert overschrijvingen van trainingspatronen op het niveau van instructieconflicten; het pakt niet de diepere vooroordelen aan die in de trainingsdata zijn ingebakken en die niet aan de oppervlakte zouden komen als instructieconflicten. Het bijbehorende Paper B-werk over Situated

Language Layers (per-tenant trainingsdiscipline, geen-gewicht-aanpassing standpunt, jurisdictiegebonden inferentie) gaat directer in op deze zorgen dan de Tractatus-kern doet.

- **Digitaal kolonialisme als een benoemd theoretisch en politiek concept.** De tenantisolatie en architecturale soevereiniteit van het voorstel zijn gedeeltelijke structurele reacties op digitaal kolonialisme; het voorstel gaat niet theoretisch in op het concept. De whitepaper Distributive Equity (waarnaar vanaf deze site wordt verwezen) gaat hier explicieter op in dan de kern van Tractatus.
- **Milieu-impact van AI** wordt grotendeels niet behandeld. De CPU-fallback-inferentiearchitectuur in de Village- implementatie is een gedeeltelijke operationele reactie; het maakt geen deel uit van de verklaarde toezeggingen van het raamwerk.

De eerlijke implicatie van deze gap-analyse is dat het voorstel de architecturale basiselementen biedt die nodig zijn om het Maori-gezag over Maori-gegevens te operationaliseren, terwijl wordt erkend dat operationalisering in te ao Maori-contexten een aanzienlijke afzonderlijke onderneming is die door kaupapa-Maori geleid ontwerpwerk vereist dat dit voorstel niet heeft gedaan. Het voorstel van de commissie in §II punt 4 is een mechanisme waarmee dat verdere werk zou kunnen worden bevorderd; het wordt aangeboden ter overweging in plaats van als een volledig antwoord.

Het Algoritmehandvest voor Aotearoa Nieuw-Zeeland, ondertekend door overheidsinstanties in 2020, biedt de bestaande basis voor transparantie, partnerschap met de Māori, eerlijkheid, verantwoordingsplicht en gegevensbescherming bij algoritmische besluitvorming door de overheid. Dit voorstel vervangt het Algoritmehandvest niet; de aanbevelingen die volgen zijn bedoeld om binnen en naast dit handvest te worden geïmplementeerd, en naast de Te Kāhui Raraunga-kaders. [CITATIE: Algoritmehandvest voor Aotearoa Nieuw-Zeeland (2020). https://www.data.govt.nz/leadership/governance/data-ethics/algorithm-charter/ — huidige status en eventuele latere updates in afwachting van verificatie.]

(iv) De wereldwijde traditie van inheemse gegevenssoevereiniteit

Inheemse gegevenssoevereiniteit is een internationale beweging, geen Nieuw-Zeelandse eigenaardigheid. Het benoemen van de internationale traditie is belangrijk: het plaatst het op Te Tiriti gebaseerde werk hierboven in een mondiaal gesprek in plaats van als bekrompen lokalisme, en het creëert een gemeenschappelijke basis met de auteurs van het CAC-kader als medebijdragers aan niet-westerse kaders voor hoe data en AI moeten worden beheerd.

Het **First Nations Information Governance Centre** (FNIGC) in Canada hanteert de **OCAP-principes** — Eigendom, Controle, Toegang, Bezit — die oorspronkelijk in de jaren negentig werden geformuleerd in het kader van de First Nations Regional Longitudinal Health Survey en die inmiddels zijn verankerd in de praktijk van de onderzoeksethiek bij Canadese universiteiten, overheden en First Nations-gemeenschappen. [CITATIE: First Nations Information Governance Centre. The First Nations Principles of OCAP®. https://fnigc.ca/ocap-training/]

Het **United States Indigenous Data Sovereignty Network** (USIDSN), opgericht in 2016 in samenwerking met het Native Nations Institute aan de Universiteit van Arizona, heeft de praktijk van inheemse gegevenssoevereiniteit in de Amerikaanse context bevorderd, onder meer door betrokkenheid bij federale gegevensbeleidsprocessen in de VS. [CITATIE: United States Indigenous Data Sovereignty Network. https://usindigenousdata.org/]

Het **Maiam nayri Wingara Indigenous Data Sovereignty Collective** in Australië — de naam betekent “Many Voices One Mind” — werd opgericht in 2017 en publiceerde in 2018 een Indigenous Data Sovereignty Communiqué dat de Australische praktijk op het gebied van inheemse gegevens heeft gevormd. [CITATIE: Maiam nayri Wingara Indigenous Data Sovereignty Collective. (2018). Indigenous Data Sovereignty Communiqué.]

De **Global Indigenous Data Alliance** (GIDA) coördineert internationaal tussen deze en andere nationale netwerken voor inheemse gegevenssoevereiniteit; het is onder haar auspiciën dat de CARE-principes zijn gepubliceerd. [CITATIE: Global Indigenous Data Alliance. https://www.gida-global.org/]

Dat zo veel van het filosofische zware werk in dit voorstel terug te voeren is op inheems wetenschappelijk onderzoek, is geen toeval. De terugkerende vragen — onder wiens gezag handelen gegevens en de actoren die ermee werken? aan wie zijn verantwoording en herkomst verschuldigd? wat is de juiste schaal waarop collectieve belangen worden afgewogen tegen individuele? — zijn vragen waar Indigenous Data Sovereignty al decennia aan werkt. Verzet tegen extractieve big-tech-architecturen en het formuleren van architecturale alternatieven die zijn gebaseerd op collectief gezag, is een van de meest vruchtbare bijdragen van de internationale beweging. De aanbevelingen die hierna volgen, bouwen voort op deze traditie en zijn in dialoog hierop gericht.

(v) ISO/IEC JTC 1/SC 42: het internationale landschap van AI-normen

Internationaal AI-normenwerk, gecoördineerd via ISO/IEC JTC 1/SC 42, biedt de formele terminologie en de kaders voor managementsystemen waarin dit soort aanbevelingen in de organisatiepraktijk kunnen worden geïmplementeerd. Vier normen zijn bijzonder relevant.

ISO/IEC 22989:2022 specificeert de concepten en terminologie van kunstmatige intelligentie. We gebruiken de terminologie van ISO/IEC 22989 waar deze compatibel is — de term “AI-systeem” heeft bijvoorbeeld de definitie uit 22989. De consistentie in terminologie maakt dit voorstel leesbaar voor recensenten die strikt de normen volgen en implementeerbaar naast ander werk dat is afgestemd op 22989. [CITATIE: ISO/IEC 22989:2022. Informatietechnologie — Kunstmatige intelligentie — Concepten en terminologie van kunstmatige intelligentie. Internationale Organisatie voor Normalisatie / Internationale Elektrotechnische Commissie.]

ISO/IEC 23053:2022 stelt een raamwerk vast voor AI- systemen die gebruikmaken van machine learning, waarbij de componenten van een op machine learning gebaseerd AI-systeem en de relaties daartussen in kaart worden gebracht. Aanbevelingen in dit voorstel die betrekking hebben op de levenscyclus, herkomst of attestatie op componentniveau kunnen worden geïmplementeerd naast de 23053-levenscyclusfasen. [CITATIE: ISO/IEC 23053:2022. Kader voor kunstmatige-intelligentiesystemen (AI) die gebruikmaken van machine learning (ML). ISO/IEC.]

ISO/IEC 23894:2023 biedt richtlijnen voor AI-risicobeheer. Het is de tegenhanger van de norminstantie voor de aanbevelingen van het raamwerk inzake risicomonitoring en incidentafhandeling per installatie. [CITATIE: ISO/IEC 23894:2023. Informatietechnologie — Kunstmatige intelligentie — Richtlijnen voor risicobeheer. ISO/IEC.]

ISO/IEC 42001:2023 specificeert eisen voor een AI- beheersysteem. Het is de AI-tegenhanger van ISO/IEC 27001 (informatiebeveiligingsbeheer) en ISO 9001 (kwaliteitsbeheer). Wij positioneren de aanbevelingen in dit voorstel als implementeerbaar binnen een managementsysteem in de stijl van ISO/IEC 42001; organisaties die enig onderdeel van dit voorstel overnemen, zijn waarschijnlijk organisaties die reeds werken met, of van plan zijn te gaan werken met, een op ISO/IEC 42001 afgestemd bestuurssysteem. [CITATIE: ISO/IEC 42001:2023. Informatietechnologie — Kunstmatige intelligentie — Managementsysteem. ISO/IEC.]

Bij het commissiewerk dat deze normen oplevert, zijn nationale spiegelcommissies in talrijke rechtsgebieden betrokken, waaronder het Verenigd Koninkrijk (via de British Standards Institution) en andere nationale normalisatie-instellingen wereldwijd. De deelname van Aotearoa Nieuw-Zeeland aan het werk van SC42 — via Standards New Zealand of een spiegelcommissie die voor dat doel is opgericht — is een van de fora waar de constructieve

bijdrage die dit voorstel bepleit, op natuurlijke wijze zou plaatsvinden. [OPMERKING: het bestaan van een huidig NZ SC42-spiegelcomité moet worden geverifieerd alvorens de paragraafontwerpen van de punten 4, 12, 14, 35 en 38 worden opgesteld.]

Afsluiting

Deze vijf tradities — Tractatus, CARE, op Te Tiriti gebaseerde wetenschap over inheemse gegevenssoevereiniteit, de wereldwijde beweging voor inheemse gegevenssoevereiniteit en ISO/IEC SC42 — komen samen in de architecturale keuzes die in de rest van dit voorstel worden gespecificeerd. Soevereiniteit als attributie; bilaterale federatie als coördinatie; polycentrisch bestuur als gezagsstructuur; cryptografische herkomst als auditinfrastructuur: geen van deze is voor dit voorstel uitgevonden. Elk heeft wortels in een of meer van de hierboven genoemde tradities. Wat dit voorstel bijdraagt is een specifieke ordening van deze basiselementen, aangepast aan de Aotearoa Nieuw-Zeelandse context, aangeboden als een constructieve parallel aan het raamwerk waarmee het zijn structuur deelt.

---

§I. Basisprincipes

We stellen vier basisprincipes voor voor de soevereine en gefedereerde ontwikkeling van intelligente agenten in Aotearoa Nieuw-Zeeland. Elk principe loopt parallel met een van de vier principes waarmee de *Implementatierichtlijnen* 2026 van de Cyberspace Administration of China beginnen; in elk geval bevestigen we de onderliggende intentie van het principe en bieden we een constructieve parallel die is gegrondvest op de §0-fundamenten.

Soevereiniteit en toerekenbaarheid. Elke handeling van een intelligente agent met betrekking tot een record is toe te rekenen aan een soevereine houder van dat record; de herkomst is cryptografisch; veiligheid vloeit voort uit de autoriteit van de recordhouder over zijn eigen records. Wij bevestigen de toewijding van het CAC- kader aan veiligheid en controleerbaarheid als fundamenteel. Wij stellen, als constructieve parallel, voor dat voor de Aotearoa Nieuw-Zeelandse context — waar het Te Tiriti-partnerschap, het bestaande Privacy Act 2020- kader en de CARE-toezegging inzake bevoegdheid tot controle samenkomen — op attributie gebaseerde soevereiniteit zeer geschikt is om die zelfde veiligheidskwesties te operationaliseren. De Tractatus-primitief voor grenshandhaving biedt het architecturale mechanisme; cryptografisch ondertekende records bieden het controlespoor; en de legitieme autoriteit over beide is de houder van de records, op grond van jurisdictie en partnerschapsverplichtingen. *(Parallellen met CAC §I principe 1 “veiligheid en controleerbaarheid”.)* [BRONVERMELDINGEN: Tractatus-grenshandhaving (Stroh 2026, CC BY 4.0); CARE-principes, Authority to control-verbintenis (Carroll et al. 2020); Privacywet 2020 (NZ), principes inzake informatieprivacy.]

Bilateraal en gefedereerd. Coördinatie tussen soevereine installaties vindt plaats via bilaterale federatie en open internationale standaarden. Wij erkennen de verdienste van het CAC-kader wat betreft de toewijding aan gestandaardiseerde en ordelijke ontwikkeling; standaardisatie en orde zijn noodzakelijke voorwaarden voor elke grootschalige implementatie van agentische AI , en het gecoördineerde standaardisatieprogramma van het CAC-kader is een geloofwaardige aanpak. Wij stellen voor, voor de Aotearoa Nieuw- Zeeland — kleinschaliger, gevestigde Māori-principes inzake gegevenssoevereiniteit , bestaande bilaterale institutionele afspraken tussen overheidsinstanties , hapū, iwi, maatschappelijke organisaties en de particuliere sector — dat een gefedereerde aanpak van coördinatie zeer geschikt is. Federatie tussen soevereine installaties wordt goed ondersteund door bestaande W3C-, IETF- en ISO/IEC SC42-conforme standaarden. Wij stellen bilaterale federatie ter overweging voor als een parallelle architectuur die kan samenwerken met centrale registratiebenaderingen in andere rechtsgebieden, en wij nodigen uit tot de

vorming van commissies onder geschikte overkoepelende organisaties om de dialoog over interoperabiliteit te ontwikkelen. *(Parallellen met CAC §I principe 2 "gestandaardiseerde en ordelijke ontwikkeling".)* [BRONVERMELDINGEN: W3C Decentralized Identifiers (DIDs) v1.0 (W3C-aanbeveling, 2022) en W3C Verifiable Credentials Data Model v1.1; ActivityPub (W3C-aanbeveling, 2018); ISO/IEC 42001:2023 managementsystemen; Te Kāhui Raraunga Māori AI Governance Framework + Taiuru kritische analyse (zie §0(iii)).]

Pluralistische beraadslaging, polycentrisch. Meerdere waardekaders bestaan naast elkaar binnen en tussen soevereine instellingen; de beraadslaging tussen hen is procedureel en gestructureerd; innovatie ontstaat uit lokale aanpassing onder lokaal gezag. Wij bevestigen de toewijding van het CAC- kader aan innovatiegedreven ontwikkeling. Wij stellen, als een constructieve parallel, voor dat polycentrisch bestuur — meerdere loci van gezag, meerdere waardekaders die in productieve spanning staan, met gestructureerde beraadslaging wanneer conflicten ontstaan — goed aansluit bij de Aotearoa Nieuw-Zeelandse context van het Te Tiriti-partnerschap, en goed wordt ondersteund door internationale wetenschappelijke literatuur over polycentrisch bestuur (met name het baanbrekende werk van Elinor Ostrom). De Tractatus pluralistische-beraadslaging-primitief biedt het architecturale mechanisme voor het faciliteren van beraadslaging tussen meerdere belanghebbenden wanneer grenshandhaving een waardenconflict aan het licht brengt; fundamenteel pluralisme is de filosofische toewijding die dit tot een structureel kenmerk van het kader maakt. *(Parallellen met CAC §I principe 3 "innovatiegedreven ontwikkeling".)* [BRONVERMELDINGEN: Tractatus-primitief voor pluralistische deliberatie (Stroh 2026, CC BY 4.0); Ostrom, E. (2010). Beyond Markets and States: Polycentric Governance of Complex Economic Systems. American Economic Review, 100(3), 641–672. https://doi.org/10.1257/aer.100.3.641 — volledige bibliografische gegevens moeten worden geverifieerd vóór publicatie van v1.]

Toepassingsgericht, onderbouwd. Toepassingen van intelligente agenten worden onderbouwd door implementatie in gemeenschappen die ze hebben geadopteerd; voor een voorstel uit het maatschappelijk middenveld is de juiste bewijsbasis implementatie in de praktijk. Wij bevestigen de toewijding van het CAC-raamwerk aan toepassingsgerichte ontwikkeling. Wij stellen, als constructieve parallel, voor dat voor een voorstel uit het maatschappelijk middenveld dat afkomstig is van één enkel bedrijf, bewijs van implementatie vooraf moet gaan aan een aanbeveling. Waar dit voorstel voorbeelden van implementatie in Aotearoa Nieuw-Zeeland aanhaalt (in §IV en §V) — in parochie- en hapū/iwi-contexten, in iwi- en diaspora-familiegeschiedeniscontexten, in contexten van kleine bedrijven — hebben die verwijzingen betrekking op daadwerkelijke implementaties, waarbij concrete implementatiegegevens (aantallen, startdata, reikwijdte) moeten worden toegevoegd vóór de publicatie van v1. Waar het voorstel aanbevelingen doet voor sectoren waarin MDSL nog niet is geïmplementeerd, worden die aanbevelingen geformuleerd als voorwaarden voor de soevereiniteitsarchitectuur voor elke implementatie door een actor in die sector, gericht aan iedereen die de architectuur daar zou willen toepassen. Wat implementatie aantoont, is niet alleen het aantal adopties, maar ook de architecturale beschikbaarheid — dat de substratprimitieven (cryptografische herkomst, federatie-enveloppen, lidgestuurde overdraagbaarheid, grenshandhaving) functioneren zoals gespecificeerd in reële omstandigheden met de gegevens van gemeenschappen die de proef hebben geautoriseerd, in plaats van in kunstmatige benchmarks. *(Parallellen met CAC §I principe 4 "toepassingsgestuurde aanpak".)* [CITATEN: Bewijs van MDSL-implementatie — Village (parochie- en gemeenschapscontexten), familiegeschiedenis (iwi- en diaspora-contexten), sydigital (contexten van kleine bedrijven); specifieke implementatiegegevens (aantallen, startdata, omvang van het gebruik) in afwachting van door de operator geverifieerde cijfers vóór de publicatie van v1.]

§II. Grondslagen voor soevereine ontwikkeling

Waar het kader van de Cyberspace Administration of China de technologische fundamenten consolideert onder een door de staat gecoördineerd standaardisatieprogramma, bieden wij fundamenten die geworteld zijn in cryptografische soevereiniteit en bilaterale protocollen. De twee volgende subparagrafen — het versterken van het soevereiniteitsfundament en het vaststellen van bilaterale protocollen — specificeren samen de architecturale primitieven waarop de rest van het voorstel is gebaseerd.

(I) Versterking van de soevereiniteitsbasis

Punt 1. Ontwikkel soevereine basiselementen voor agents. Cryptografisch ondertekende records, identiteitscodes die door leden kunnen worden meegenomen, en herkomstgegevens met attributen vormen de basis voor de activiteiten van agents met betrekking tot soevereine gegevens. Het zijn architecturale basiselementen die soevereiniteit op het niveau van het record zelf waarborgen. Wij stellen voor om blijvend te investeren in open-source cryptografische primitieven — digitale ondertekening, verifieerbare referenties, op inhoud gebaseerde opslag met herkomst — en in standaarden voor overdraagbare identiteit die bruikbaar zijn in elke soevereine installatie in elke sector. Wij stellen voor dat deze primitieven worden ontwikkeld en onderhouden als gemeenschappelijke infrastructuur, beschikbaar onder permissieve open-source licenties (Apache 2.0, EUPL-1.2 of compatibel), waardoor toepassing, wijziging en herdistributie door elke partij mogelijk is. De Tractatus primitief voor grenshandhaving, de primitief voor kruisverwijzingsvalidatie en de primitief voor instructie-persistentie-classificatie specificeren samen de runtime-mechanismen; cryptografische ondertekening en infrastructuur voor verifieerbare referenties bieden het onderliggende controlespoor. *(Parallellen met CAC-punt 1 “versterken van R&D in fundamentele technologieën”.)* [BRONVERMELDINGEN: Tractatus-framework (Stroh 2026, CC BY 4.0 tekst / Apache 2.0 code); W3C Decentralized Identifiers (DIDs) v1.0 (W3C-aanbeveling, 2022); W3C Verifiable Credentials Data Model v1.1; CARE-principes, Authority-to-control-verbintenis (Carroll et al. 2020).]

Punt 2. Verfijn de soevereine toolchain. Open-source referentie-implementaties van agent-frameworks — inclusief de zes diensten van het Tractatus-framework — moeten beschikbaar zijn voor gebruik door elke soevereine installatie onder permissieve open-source licenties die installatielokale werking toestaan. Wij stellen voor dat de toolchain voor het ontwikkelen, testen, implementeren en onderhouden van op soevereiniteit gebaseerde agentische systemen in het openbaar wordt ontwikkeld, waarbij bijdragen van elke soevereine installatie worden aangemoedigd. De huidige MDSL-implementaties — het Tractatus-framework gedistribueerd onder Apache 2.0 (met documentatie onder CC BY 4.0); de Village- en community-codebases die vanaf medio 2026 EUPL-1.2 in fasen vanaf medio 2026 — worden aangeboden als één set referentie-implementaties van de potentieel vele. Beveiligingstools — detectie van vijandige invoer, detectie van gedragsafwijkingen, attestatietools voor builds en afhankelijkheden — vormen de passende technische aanvulling op de Tractatus-primitieven voor grenshandhaving en metacognitieve verificatie. *(Parallellen met CAC-punt 2 “verfijnen van de agent-toolchain”.)* [CITATEN: Tractatus-framework referentie-implementatie (Stroh 2026), Apache 2.0 (code), CC BY 4.0 (tekst en figuren); EUPL-1.2 (European Union Public Licence); Apache 2.0 (Apache Software Foundation).]

(II) Het opstellen van bilaterale protocollen

Punt 3. Gefedereerde bilaterale protocollen. Interoperabiliteit tussen soevereine installaties vindt plaats via bilaterale overeenkomsten en open internationale standaarden. Wij erkennen de verdienste van de toewijding van het CAC-raamwerk aan een gestandaardiseerd interconnectieprogramma — het voorgestelde Intelligent Agent Interconnection Protocol

(AIP), fundamentele interfacestandaarden voor software, diensten en hardware-randapparatuur, en verplichte standaarden in gevoelige sectoren. Wij stellen voor, in de context van Aotearoa Nieuw-Zeeland, dat interoperabiliteit tussen soevereine installaties goed wordt ondersteund door het bestaande landschap van internationale standaarden: W3C Decentralized Identifiers en Verifiable Credentials voor identiteit; ActivityPub en gerelateerde W3C-federatieprotocollen voor communicatie tussen installaties; IETF-protocollen voor authenticatie, transport en contentadressering; en ISO/IEC SC42-werk voor AI-specifieke terminologie, levenscyclus, risico en afstemming van beheersystemen. Wij stellen voor dat Aotearoa NZ bijdraagt aan internationale interoperabiliteitsnormen als gelijkwaardige deelnemer aan die bestaande fora. *(Parallellen met CAC-punt 3 "standaardisatiesysteem" en het voorgestelde AIP-interconnectieprotocol.)* [CITATEN: W3C DIDs v1.0; W3C Verifiable Credentials Data Model v1.1; ActivityPub (W3C-aanbeveling, 2018); ISO/IEC 22989:2022 terminologie; ISO/IEC 23053:2022 ML-raamwerk.]

Punt 4. Cryptografische identiteit; federatieve dialoog over het Intelligent Internet. Identiteit is per installatie, verankerd in DNS en cryptografische sleutels; verificatie tussen tegenpartijen is peer-to-peer; capaciteitsverklaringen worden door elke installatie gepubliceerd. Wij erkennen de verdienste van het voorstel van het CAC-kader voor een registratieplatform voor intelligente agenten, dat niet alleen voorziet in digitaal identiteitsbeheer en capaciteitsverklaringen, maar ook in zoeken en ontdekken, betrouwbare interconnectie, conforme betaling, beveiliging, conflictoplossing, gebruik van IPv6 en een monitoringsysteem — een substantiële en samenhangende reeks onderling gerelateerde functies. Een gecentraliseerd registratieplatform met een coördinerende autoriteit is een geloofwaardige architecturale benadering van deze functies.

Wij stellen voor, voor de context van Aotearoa Nieuw-Zeeland — waar kleinschalige, gevestigde Maori-principes van gegevenssoevereiniteit en de architecturale primitieven die al vertegenwoordigd zijn in MDSL-implementaties samenkomen — een gefedereerde aanpak waarin elke Intelligent Internet- functie wordt aangepakt via bilaterale afspraken en open internationale standaarden. Identiteits- en capaciteitsverklaringen worden verzorgd door W3C Decentralized Identifiers en Verifiable Credentials. Zoeken en ontdekken tussen soevereine installaties kan gebruikmaken van de patronen die zijn vastgesteld door van ActivityPub afgeleide federatie, door WebFinger (IETF RFC 7033) en door federatiebewuste directoryprotocollen zoals nodeinfo — hoewel we opmerken dat gefedereerd ontdekken op schaal een open technisch probleem blijft en dit als zodanig erkennen. Betrouwbare interconnectie en beveiliging werken via bilaterale cryptografische attestatie. Conforme betalingsroutes via bestaande financiële regelgevingskanalen. Conflictoplossing werkt via bilaterale bemiddeling en bestaande mechanismen voor geschillenbeslechting, waarbij cryptografische herkomst het controlespoor vormt. IPv6 is een onderliggende infrastructuurkeuze die beschikbaar is voor elke installatie. Een systeem van monitoringindicatoren is realiseerbaar door open publicatie van operationele statistieken door elke deelnemende installatie, geaggregeerd door onafhankelijke waarnemers.

Wij stellen voor om één commissie op te richten onder een geschikte overkoepelende organisatie — kandidaten zijn onder meer de Royal Society Te Apārangi, de Standards New Zealand SC42-spiegelcommissie (bestaan te verifiëren), het New Zealand AI Forum, of een gezamenlijke structuur van deze — **om gedetailleerde aanbevelingen in de NZ-context te ontwikkelen voor agentische AI-architectuur, om bij te dragen aan het werk van ISO/IEC JTC 1/SC 42 als gelijkwaardige deelnemer, en om een bilaterale dialoog aan te gaan met de auteurs van het CAC- kader en met internationale collega's. De commissie zou vijf benoemde werkstromen uitvoeren: (i) federatieve identiteit voor intelligente agenten en de bredere Intelligent Internet-functies genoemd in dit punt; (ii) federatieve audit- en nalevingsdiensten (zie §III punt 12); (iii) op attestatie gebaseerde reputatiesystemen (zie §III punt 14); (iv) patronen voor coördinatie binnen de sector, waaronder federatie- versus alliantie-modellen**

(zie §V punt 35); en (v) internationale betrokkenheid en bilaterale samenwerking op het gebied van agentische AI (zie §V punt 38). De bijdrage van de commissie aan internationaal normalisatiewerk en aan de dialoog met de auteurs van het CAC-kader is haar belangrijkste resultaat. Wij bieden dit commissievoorstel aan als een bijdrage aan de internationale dialoog; de dialoog zal baat hebben bij bijdragen uit vele architecturale tradities. *(Parallellen met CAC-punt 4 "intelligente internetarchitectuur" met registratieplatform; het patroon voor commissievorming is geconsolideerd in de punten 4, 12, 14, 35 en 38.)* [CITATEN: W3C Decentralized Identifiers (DIDs) v1.0; W3C Verifiable Credentials Data Model v1.1; ActivityPub (W3C-aanbeveling 2018); WebFinger (IETF RFC 7033); nodeinfo federatie-directory; ISO/IEC 22989:2022; Te Kāhui Raraunga (kahuiraraunga.io — Māori-model voor gegevensbeheer en Māori-kader voor AI-beheer); Taiuru, K. (20 sep 2025) Kritische analyse van de Te Mana Raraunga-gegevensprincipes, taiuru.co.nz/critical-analysis-mana-raraunga/; Royal Society Te Apārangi; ISO/IEC JTC 1/SC 42.]

---

§III. Handhaving van de soevereiniteitsbasis

Waar het kader van de Cyberspace Administration of China een veiligheidsbasislijn vaststelt via productrichtlijnen, behavioral-fencing-technologieën, gelaagde governance en zelfregulering door de sector met kredietwaardigheidssancties, bieden wij een basislijn die geworteld is in het eigen jurisdictionele kader van de gebruiker, cryptografische herkomst, polycentrische governance-regelingen en op federatie gebaseerde coördinatie. De vier volgende subparagrafen — productprincipes, veiligheidsrisico's, bestuurssysteem, federatieve coördinatie — specificeren samen hoe de naleving van soevereiniteitsprincipes door een intelligente agent kan worden geverifieerd tijdens de uitvoering en achteraf gecontroleerd.

(I) Verduidelijking van productprincipes

Punt 5. Verankering in de eigen wetgeving van de gebruiker. Beleid, regelgeving en ethische normen met betrekking tot intelligente agenten vloeien voort uit het rechtsgebied van de gebruiker. Waarden zijn afkomstig uit lokale wetgeving en lokale institutionele regelingen; de architectuur biedt de implementatie-infrastructuur waarin die waarden van kracht zijn. In Aotearoa Nieuw-Zeeland omvatten de toepasselijke instrumenten de Privacywet 2020 (met de Health Information Privacy Code 2020 en andere codes voor specifieke sectoren); de New Zealand Bill of Rights Act 1990 wanneer overheidsactoren betrokken zijn; het Algorithm Charter for Aotearoa New Zealand voor overheidsinstanties; de verplichtingen uit het Te Tiriti o Waitangi voor overheidsactoren en de daaruit voortvloeiende partnerschapsverplichtingen; de Official Information Act 1982; de Public Service Act 2020; de Public Records Act 2005; en sectorale wetten, waaronder de Reserve Bank of New Zealand Act 2021, de Education and Training Act 2020, de Local Government Act 2002 en de Search and Surveillance Act 2012, die van toepassing zijn op de relevante implementatiecontext. De architectuur is implementatieneutraal met betrekking tot de vraag welke jurisdictie van toepassing is; het voorstel is gericht aan gebruikers in Aotearoa NZ, en dezelfde primitieven dienen gebruikers in elke jurisdictie waarvan zij de waarden willen operationaliseren. *(Parallellen met CAC-punt 5 "beleid, regelgeving en ethische normen".)* [CITATEN: Privacywet 2020 (NZ); Nieuw-Zeelandse Bill of Rights Act 1990; Algoritmehandvest voor Aotearoa Nieuw-Zeeland (2020); Health Information Privacy Code 2020; Official Information Act 1982; Public Service Act 2020; Public Records Act 2005; Reserve Bank of New Zealand Act 2021; Education and Training Act 2020; Local Government Act 2002; Search and Surveillance Act 2012 — huidige wetgevingsversies moeten worden geverifieerd vóór publicatie van v1.]

Punt 6. Uiteindelijke beslissingsbevoegdheid van de gebruiker, cryptografisch onderbouwd. Wij bevestigen hetzelfde principe dat het CAC-raamwerk bevestigt: de gebruiker behoudt het recht om geïnformeerd te worden over, en de uiteindelijke beslissingsbevoegdheid te hebben over, autonome acties die door intelligente agenten namens hem of haar worden ondernomen. Dit principe vormt de basis voor de vertrouwensrelatie tussen een persoon en de agentsystemen die namens hem handelen. Wij stellen als controlemechanisme voor: cryptografische herkomst per record ten opzichte van het eigen soevereine record van de gebruiker: elke autonome handeling door een agent die op basis van de records van de gebruiker opereert, produceert een cryptografische vermelding die de handeling bevestigt, toeschrijfbaar aan de agent en aan het autorisatiekader van de gebruiker. De gebruiker kan elke actie van een agent inspecteren, terugkijken en betwisten aan de hand van deze herkomst, en de Tractatus-primitief voor instructie-persistentie-classificatie biedt het kader om routinematige acties te onderscheiden van acties die expliciete herbevestiging door de gebruiker vereisen. *(Parallellen met CAC-punt 6 “verduidelijking van de beslissingsbevoegdheid”.)* [CITATEN: Tractatus-primitief voor instructie-persistentie-classificatie (Stroh 2026, CC BY 4.0); Privacywet 2020 (NZ), informatieprivacybeginsel 6 (toegangsrechten); CARE-principes, toezeggingen inzake bevoegdheid tot controle (Carroll et al. 2020).]

Punt 7. Herkomst, als aanvulling op gedragscontrole. We erkennen de nadruk die het CAC-raamwerk legt op inbedding van regels, gedragsbeperking en blockchain-verankerde verificatie van agentgedrag in kritieke toepassingsscenario’s. Dit zijn geloofwaardige architecturale benaderingen om wettig en conform gedrag te waarborgen in centraal gecoördineerde implementaties. Wij stellen, als een aanvullende architecturale primitief die zeer geschikt is voor bilaterale federatie, **herkomst** voor: elke actie van een intelligente agent levert een cryptografisch record op dat aan de actor kan worden toegeschreven. De twee benaderingen vullen elkaar aan. Gedragsbeperking beperkt wat een agent tijdens de uitvoering mag proberen; herkomst creëert een onvervalsbaar verslag van wat daadwerkelijk is geprobeerd. Beide hebben een rol, en de juiste balans tussen beide is waarschijnlijk contextspecifiek. *(Parallellen met CAC-punt 7 “versterking van gedragscontrole”.)* [BRONVERMELDINGEN: Tractatus-primitief voor validatie van kruisverwijzingen (Stroh 2026, CC BY 4.0); W3C Verifiable Credentials Data Model v1.1; ISO/IEC 23894:2023 risicobeheer.]

(II) Beperken van beveiligingsrisico's Risico's

Punt 8. Intrinsieke beveiliging door middel van soevereine primitieven. Persoonsgegevens blijven op de installatie van de houder; de cryptografische beveiliging is zowel per record als perimetergebaseerd; aanvalsdetectie vindt lokaal plaats op de records van de houder; toegang is contractueel vastgelegd tussen tegenpartijen. De impact van een storing blijft beperkt tot de betrokken installatie. Wij bevestigen de toewijding van het CAC-raamwerk aan intrinsieke beveiligingsmogelijkheden — gegevensbeveiliging, bescherming van persoonlijke informatie, cryptografische bescherming, aanvalsdetectie, toegangscontrole, gedragscontrole. Wij stellen, als een constructieve parallel, voor dat voor een gefedereerde architectuur de juiste locatie van deze mogelijkheden de soevereine installatie is, met bilaterale mechanismen voor samenwerking tussen installaties wanneer bedreigingen jurisdictionele of organisatorische grenzen overschrijden. *(Parallellen met CAC punt 8 “intrinsieke beveiligingscapaciteiten”.)* [BRONVERMELDINGEN: Tractatus boundary enforcement primitive (Stroh 2026, CC BY 4.0); Privacy Act 2020 (NZ); ISO/IEC 23894:2023 risicobeheer.]

Punt 9. Supply-chain-attestatie, federatief delen. Wij stellen per installatie attestatie over de volledige levenscyclus voor — ondertekende build- herkomst, afhankelijkheidsmanifesten, attestatie van trainingsgegevens waar van toepassing, geschiedenis van reacties op beveiligingsincidenten — openbaar gepubliceerd door elke installatie. Supply-chain-

incidenten worden bilateraal gedeeld tussen federatieve peers en via gevestigde internationale kanalen, waaronder CERT-NZ, CERT-EU, US-CERT en het CVE-coördinatiesysteem. Wij erkennen de verdienste van de toewijding van het CAC-raamwerk aan beveiligingsnormen voor de volledige levenscyclus en het delen van informatie over de toeleveringsketen. Wij stellen voor dat voor gecoördineerde samenwerking de transparantie van de toeleveringsketen wordt bereikt door middel van openbare publicatie van attesten door elke installatie, met bilaterale samenwerking bij de respons op incidenten. *(Parallellen met CAC-punt 9 "beveiliging van de toeleveringsketen".)* [BRONVERWIJZINGEN: ISO/IEC 23894:2023 risicobeheer; CERT-NZ-openbaarmakingsprocedures; internationaal CVE-coördinatieproces; ISO/IEC 42001:2023 managementsystemen.]

Punt 10. Beperk de schadebereik; controleer achteraf. Routinematige risico-identificatie vindt lokaal plaats bij elke installatie, waarbij incidenten die meerdere installaties betreffen zich via de federatie verspreiden. De belangrijkste bijdrage van het kader aan het beperken van het risico op geautomatiseerde aanvallen, inbreuken op de privacy en de verspreiding van valse informatie is het beperken van de schaal waarop geautomatiseerde schade zich opstapelt. Wij bevestigen de toewijding van het CAC- kader aan risico-identificatie, vroegtijdige waarschuwing, interventie en het voorkomen dat agentische AI wordt gebruikt voor illegale activiteiten (geautomatiseerde aanvallen, inbreuken op de privacy, het genereren en verspreiden van valse informatie, online fraude). Wij stellen voor, als een aanvullende architecturale bijdrage, dat het beperken van de omvang van geautomatiseerde schade — door middel van operationele grenzen per installatie en bilaterale samenwerking bij incidentrespons — een structurele aanvulling vormt op detectie- en interventiebenaderingen op gecentraliseerd niveau. Het structurele mechanisme is de **federatie-envelop**: standaard blijven de records van een installatie binnen die installatie, en stroomt er alleen informatie tussen installaties via enveloppen die de installatie expliciet ondertekent, met vermelding van herkomst en ontvanger. Compromittering van één installatie kan zich niet ongemerkt verspreiden naar andere, omdat het substraat geen impliciet leespad tussen installaties heeft — er is geen gedeeld register waar een aanvaller gebruik van kan maken. Bilaterale incidentrespons werkt dan op wat opzettelijk is gedeeld, waarbij de herkomst van de federatie-envelop forensische reconstructie van de getroffen omvang mogelijk maakt zonder dat een gecentraliseerde auditaggregator nodig is. *(Parallellen met CAC-punt 10 "risico's als gevolg van toepassingen beperken".)* [BRONVERMELDINGEN: Tractatus pluralistic deliberation primitive (Stroh 2026, CC BY 4.0); ISO/IEC 23894:2023 risicobeheer; Privacy Act 2020 (NZ); Harmful Digital Communications Act 2015 (NZ) — huidige wetgevingsversies moeten worden geverifieerd vóór publicatie van v1.]

(III) Verbetering van het governancesysteem

Punt 11. Polycentrisch bestuur, in dialoog met gelaagde benaderingen. De bestuursbevoegdheid over wat een intelligente agent met een record mag doen, berust bij de houder van de records. De toelaatbaarheid van scenario's wordt per installatie bepaald door de eigen jurisdictie van de houder, ondersteund door sectorale toezichthouders waar hun bevoegdheid zich uitstrekt tot het relevante onderwerp. Wij erkennen de verdiensten van de gecategoriseerde en gelaagde bestuursaanpak van het CAC-kader voor gevoelige sectoren en sleutelindustrieën, waarbij de Cyberspace Administration of China en relevante industriële autoriteiten toelaatbare toepassingsscenario's bepalen en beheersmaatregelen implementeren zoals registratie, testen en het terugroepen van problematische producten. Wij stellen voor, in de context van Aotearoa Nieuw Zeeland, dat polycentrisch bestuur — meerdere bevoegdheidscentra verspreid over overheidsinstanties, hapū/iwi-entiteiten, sectorale regelgevers, beroepsorganisaties en de houders van de gegevens zelf — goed aansluit bij het bestaande institutionele landschap en bij de partnerschapsverplichtingen uit het Verdrag van Waitangi. Internationaal wetenschappelijk onderzoek naar polycentrisch bestuur, met name het baanbrekende werk van Elinor Ostrom, biedt de theoretische

onderbouwing voor deze aanpak. Polycentriciteit wordt operationeel ondersteund door de eigenschappen van het substraat: één enkele **cryptografisch ondertekende auditketen** per record stelt meerdere autoriteiten — de regelgevende instantie van de Kroon, de hapū/iwi-entiteit, de sectorale instantie, de beroepsorganisatie, de recordhouder zelf — in staat om elk hetzelfde record te verifiëren binnen hun respectieve bevoegdheid, zonder dat er gecentraliseerde verzameling of dubbele registers nodig zijn. Verschillende autoriteiten bewaren hun eigen kopieën van de auditketen onder hun eigen sleutels en komen tot onafhankelijke nalevingsbeoordelingen van hetzelfde onderliggende record. De architecturale basis die polycentrisch bestuur operationeel beheersbaar maakt, is de door de federatie gerepliceerde, ondertekende auditketen; de institutionele vraag wie bevoegdheid heeft over welke beslissingsklasse blijft politiek. *(Parallellen met CAC-punt 11 "gecategoriseerd en gelaagd bestuur".)* [CITATEN: Ostrom, E. (2010). Beyond Markets and States: Polycentric Governance of Complex Economic Systems. American Economic Review, 100(3), 641–672. https://doi.org/10.1257/aer.100.3.641; Algorithm Charter for Aotearoa New Zealand (2020); Te Kāhui Raraunga (kahuiraraunga.io – Māori Data Governance Model en Māori AI Governance Framework); Taiuru, K. (20 sep 2025) Critical Analysis of Te Mana Raraunga Data Principles, taiuru.co.nz/critical-analysis-mana-raraunga/.]

Punt 12. Gecoördineerde nalevingsdiensten. Risicobewaking, testen, evaluatie, audit en certificeringsdiensten voor intelligente agenten bestaan als commerciële, gemeenschaps- en academische aanbiedingen; wederzijdse erkenning tussen diensten vindt plaats via open publicatie en peer review. Wij erkennen de verdienste van het CAC- kader dat zich inzet voor een systeem van nalevingsdiensten dat professionele diensten biedt zoals risicomonitoring, testen en evaluatie, advies en certificering, met bevordering van wederzijdse erkenning tussen geaccrediteerde aanbieders. **Dit gebied is werkstroming (ii) van de enkele commissie voorgesteld in §II punt 4. De commissie zou aanbevelingen in de Nieuw-Zeelandse context opstellen voor een gefedereerd auditkader voor intelligente agents, bijdragen aan het werk van ISO/IEC SC42 op het gebied van AI-beoordeling, evaluatie en beheersystemen, en een bilaterale dialoog aangaan met de auteurs van het CAC-kader over de interactie tussen gefedereerde en gecentraliseerde compliance-diensten.** Compliance-diensten federeren concreet als volgt: elke installatie publiceert haar eigen attesten — build-herkomst, afhankelijkheidsmanifesten, attesten van trainingsgegevens waar van toepassing, geschiedenis van incidentrespons, naleving van het auditkader — onder haar eigen cryptografische identiteit. Compliance-aanbieders verifiëren aan de hand van deze verklaringen en publiceren hun bevindingen onder hun eigen identiteit; wederzijdse erkenning tussen aanbieders vindt plaats door middel van kruisverwijzingen naar cryptografisch verifieerbare beoordelingen in plaats van via centrale accreditatie. De basiscomponent die dit operationeel maakt, is inhoudsgerichte publicatie met cryptografische herkomst — iedereen kan elke compliance-beoordeling verifiëren aan de hand van de specifieke versie van de installatie die daadwerkelijk is beoordeeld. *(Parallellen met CAC-punt 12 "compliance-servicesysteem"; geconsolideerde werkstromen voor de vorming van commissies zijn van toepassing.)* [VERWIJZINGEN: ISO/IEC 42001:2023 managementsystemen; ISO/IEC 23894:2023 risicomanagement; Royal Society Te Apārangi.]

(IV) Versterking van de gecoördineerde samenwerking

Punt 13. Coördinatie door federatie. Soevereine installaties vormen bilaterale federaties; coördinatie over gedeelde aandachtspunten — interoperabiliteitsnormen, openbaarmaking van beveiligingsincidenten, ontwikkeling van auditkaders — vindt plaats via open publicatie en consensus onder bijdragende gelijken. Wij erkennen de verdienste van de inzet van het CAC- kader voor zelfregulering door de sector, waarbij brancheorganisaties en grote ondernemingen gezamenlijk zelfregulerende regels opstellen met betrekking tot naleving van AI-functionaliteit, algoritmebeheer, bescherming van intellectueel eigendom en eerlijke

concurrentie. Wij stellen voor, voor de gefedereerde architectuur die in dit voorstel wordt gespecificeerd, dat de coördinatie van gemeenschappelijke aandachtspunten plaatsvindt via open publicatie en consensus onder bijdragende peers; de architecturale toewijding aan bilaterale federatie strekt zich uit tot het coördinatiemechanisme zelf. Federatie is in dit voorstel per definitie bilateraal: elke installatie publiceert een federatie- eindpunt en kiest met welke peers zij zal federeren, op basis van welke specifieke recordklassen; het **federatie-envelopformaat** specificeert welke records mogen worden verzonden, met welke toestemmingsscope, naar welke ontvanger, met welke beperkingen op het doorsturen. De basiselementen die bilaterale federatie operationeel maken, zijn de federatie-envelop (een aan de ontvanger gebonden, met herkomstgegevens gekoppeld, in reikwijdte beperkt berichtformaat), **door leden gestuurde overdraagbaarheid** (de houder van records kan verzoeken om verzending vanuit elke installatie naar elke bestemming van zijn keuze), en **cryptografische herkomst** (elk record bevat verifieerbare metadata over de oorsprong die de overdracht overleeft). Coördinatie rond gedeelde aandachtspunten — interoperabiliteitsnormen, openbaarmaking van beveiligingsincidenten, ontwikkeling van auditkaders — verloopt bilateraal tussen gefedereerde peers zonder dat er een gecentraliseerd register nodig is. *(Parallellen met CAC-punt 13 “zelfregulering door de sector”.)* [BRONVERMELDINGEN: ActivityPub-federatieprotocol (W3C-aanbeveling 2018); IETF Request for Comments-proces; W3C-procesdocument.]

Punt 14. Reputatie door attestering. Soevereine installaties publiceren hun eigen attesten — beveiligingsstatus, auditgeschiedenis, afhankelijkheidsmanifesten, incidentrespons — en tegenpartijen verifiëren deze cryptografisch. Reputatie wordt opgebouwd door een geschiedenis van nauwkeurige zelfopenbaarmaking, geverifieerd door bilaterale tegenpartijen. Wij erkennen de waarde van het voorstel van het CAC-kader voor vrijwillige kredietbeoordelingsmechanismen voor marktentiteiten in de sector van intelligente agenten, met kredietbeoordelingen voor gedragingen zoals misbruik van technologie, het stimuleren van consumptie, misleidende reclame en het verbergen van informatie over defecten, en sancties voor oneerlijk gedrag in overeenstemming met wet- en regelgeving. **Dit gebied is werkstroming (iii) van de enkele commissie voorgesteld in §II punt 4. De commissie zou aanbevelingen in de context van Nieuw-Zeeland ontwikkelen over op attestatie gebaseerde reputatie versus op registers gebaseerde reputatie, bijdragen aan internationaal normwerk inzake AI-herkomst en attestatie, en een bilaterale dialoog aangaan met de auteurs van het CAC- kader over interoperabiliteit tussen op attestatie gebaseerde en op kredietbeoordeling gebaseerde reputatiesystemen.** *(Parallellen met CAC-punt 14 “kredietbeoordelingsmechanismen”; de geconsolideerde werkstroom voor de vorming van commissies is van toepassing.)* [CITATEN: W3C Verifiable Credentials Data Model v1.1; ISO/IEC 42001:2023 managementsystemen.]

---

§IV. Versterking van adoptiegedreven ontwikkeling

Waar het kader van de Cyberspace Administration of China negentien sectoren opsomt waarin de staat voorschrijft dat “actoren X moeten doen”, spiegelen wij de negentien sectoren en herformuleren we elk ervan als een vraag naar soevereiniteitsvoorwaarden voor elke inzet van actoren in die sector. Het kader schrijft geen inzet voor; het specificeert de architecturale voorwaarden waaronder inzet verenigbaar is met soevereiniteit. De herformulering is retorisch bescheiden maar structureel ingrijpend: de door de staat gestuurde interpretatie positioneert intelligente actoren als instrumenten van sectorale programma’s, terwijl de interpretatie op basis van soevereiniteitsvoorwaarden hen positioneert als hulpmiddelen waarvan het gebruik moet voldoen aan eisen inzake attributie, herkomst en lid-overdraagbaarheid, ongeacht wie ze inzet.

De architecturale primitieven die in de negentien sectoren die volgen worden aangeroepen,

zijn vier. **Cryptografische herkomst** koppelt verifieerbare metadata over de oorsprong aan elk record — wie het schreef, wanneer, op basis van welke bevoegdheid — onveranderbaar voor stille bewerking achteraf (correcties worden medeondertekend en zelf geregistreerd). **Federatie-enveloppen** bemiddelen bij het delen tussen installaties: alleen de goedgekeurde subset wordt verzonden, met herkomst, ontvangersbinding en geen doorsturen als standaard. **Lidgestuurde overdraagbaarheid** stelt de houder van records in staat zijn bundel naar een andere installatie te exporteren zonder toestemming van de oorspronkelijke houder, waarbij de herkomst intact blijft op de bestemming. **Handhaving van grenzen** leidt beslissingen in de vier grenscategorieën (onomkeerbaarheid, waardegeladen, afhankelijk van culturele context, ongekend) standaard naar menselijke beraadslaging, waarbij de routering zelf wordt vastgelegd. De sectoritems die volgen benoemen de sectorspecifieke manifestatie van een of meer van deze primitieven; de generieke mogelijkheden zijn constant in alle sectoren. Zie *Architectural Alignment* §3 voor de ontwikkeling van de primitieven; *Paper A* voor de volledige substraatlaag.

(I) Wetenschappelijk onderzoek

Punt 15. In onderzoek gelden soevereine basisprincipes. Onderzoeksomgevingen werken met soevereine datasets — die in het bezit zijn van deelnemende personen, instellingen, hapū/iwi-entiteiten of onderzoeksconsortia onder hun respectieve bestuursregelingen; afkomstgegevens worden bij de afgeleide resultaten gevoegd; bilaterale federatie tussen instellingen biedt de interoperabiliteitslaag waar gegevensuitwisseling noodzakelijk is. Wij erkennen de verdienste van de visie van het CAC-kader waarin intelligente agenten theoretische deductie, kennisintegratie en integratie met wetenschappelijke instrumenten en experimentele platforms versterken. Wij stellen voor dat voor onderzoek in Aotearoa NZ deze mogelijkheden worden ingezet onder een regeling voor onderzoeksethiek die specifiek is voor elke instelling en elk onderzoeksproject, waarbij de Tractatus primitieve voor pluralistische beraadslaging het architecturale mechanisme biedt voor het opschalen van de beoordeling van onderzoeksethiek over concurrerende waardenkaders heen. De operationele primitieven zijn cryptografische herkomst (elke dataset en afgeleid resultaat draagt een herkomstverklaring die de bronnen, afleidingen en het ethische beoordelingskader waaronder het is geproduceerd, bevestigt) en federatie-enveloppen (instellingoverschrijdende uitwisseling vindt plaats onder expliciete overeenkomsten voor gegevensuitwisseling, waarbij de envelop vastlegt welke subset van gegevens wordt verzonden en onder welke toestemmingsscope). Lidgestuurde overdraagbaarheid stelt een onderzoeksdeelnemer in staat zijn bijdrage in te trekken en de herkomst stroomafwaarts te laten bijwerken; grenshandhaving leidt de met waarden beladen ethische beslissingen naar de commissie voor onderzoeksethiek in plaats van naar autonome agentactie. *(Parallellen met CAC-punt 15 "onderzoek en verkenning".)* [BRONVERMELDINGEN: CARE-principes (Carroll et al. 2020); FAIR-principes (Wilkinson et al. 2016, https://doi.org/10.1038/sdata.2016.18); Te Kāhui Raraunga (kahuiraraunga.io — Māori-model voor gegevensbeheer en Māori-kader voor AI-beheer); Taiuru, K. (20 sep 2025) Kritische analyse van de Te Mana Raraunga-gegevensprincipes, taiuru.co.nz/critical-analysis-mana-raraunga/; Nieuw-Zeelands kader voor onderzoeksethiek via de Health Research Council en Royal Society Te Apārangi; Tractatus pluralistische deliberatieprimitief (Stroh 2026).]

Punt 16. In software-R&D zijn attributie en audit van toepassing. Agents voor codegeneratie werken op basis van geattribueerde bronnen; afgeleide werken dragen hun afstamming; CI/CD-pijplijnen verifiëren de bouwcertificering en de herkomst van afhankelijkheden. Wij erkennen de verdienste van de toewijding van het CAC-kader aan intelligente agents voor softwareontwikkeling die de vereistenanalyse, het architectonisch ontwerp, de codegeneratie en het testen verbeteren. Wij stellen voor dat al deze capaciteiten functioneren onder vereisten inzake attributie en herkomst; bijdragen van agents aan code,

ontwerp of simulatie-outputs worden zowel toegeschreven aan de agent als aan de menselijke of organisatorische operator op wiens gezag ze zijn geproduceerd. De operationele primitief is cryptografische herkomst toegepast op elk code-artefact — de agent die het heeft voorgesteld, de menselijke beoordelaar die het heeft goedgekeurd, de build-pijplijn die het heeft gecompileerd, de eigen attestaties van de afhankelijkheidsboom — waardoor een verifieerbare keten wordt gevormd vanaf de geschreven regel terug naar de geautoriseerde commit. De Tractatus-primitief voor kruisverwijzingsvalidatie biedt runtime-verificatie dat voorgestelde code-acties consistent zijn met de canonieke instructiegeschiedenis. *(Parallellen met CAC-punt 16 “R&D-ondersteuning”.)* [CITATEN: W3C Verifiable Credentials Data Model v1.1; SBOM-standaarden (Software Bill of Materials) via NTIA en OWASP CycloneDX; Tractatus-primitief voor validatie van kruisverwijzingen (Stroh 2026).]

(II) Industriële ontwikkeling

Punt 17. In de productie zijn soevereiniteitsprimitieven van toepassing. Productiegegevens zijn het soevereine dossier van de fabrikant; agenten die hiertegen handelen, worden geïdentificeerd; coördinatie tussen installaties voor toeleveringsketens is bilateraal. Wij erkennen de verdienste van de toewijding van het CAC-raamwerk aan productiebeheeragenten voor planning, toewijzing van middelen en procesoptimalisatie, en aan integratie met CNC-bewerkingsmachines, industriële robots en geautomatiseerde productielijnen. Wij stellen voor dat al deze mogelijkheden functioneren onder het gezag van de fabrikant, waarbij de coördinatie van de toeleveringsketen plaatsvindt via bilaterale overeenkomsten tussen deelnemende fabrikanten en tegenpartijen. De operationele basiselementen zijn cryptografische herkomst (elke batch draagt een productielijncertificaat — sensormetingen, beslissingen van agenten, menselijke goedkeuringen — achteraf verifieerbaar vanuit elk defectonderzoek) en federatie-enveloppen (coördinatie van de toeleveringsketen vindt plaats via bilateraal ondertekende enveloppen waarin wordt gespecificeerd welke productiegegevens met welke tegenpartij worden gedeeld en voor welk doel). Lidgestuurde overdraagbaarheid betekent hier het vermogen van de fabrikant om zijn volledige productie-audittrail te exporteren naar een andere toezichthouder of regelgevende instantie in de toeleveringsketen zonder toestemming van de oorspronkelijke platformleverancier. *(Parallellen met CAC-punt 17 “intelligente productie”.)* [CITATEN: ISO/IEC 42001:2023 managementsystemen; onderzoek naar NZ-normen voor productiegegevens en Industry 4.0 NZ-initiatieven is in behandeling.]

Punt 18. Op het gebied van energie en hulpbronnen zijn soevereiniteitsprincipes van toepassing. Milieugegevens, hulpbronnencatalogi en verzendingslogboeken zijn soevereine documenten van de verantwoordelijke entiteiten: de Kroon voor sommige (wettelijke hulpbronnen, bepaalde milieugegevens); hapū en iwi voor die waar toewijzingen uit de Verdragregeling van toepassing zijn; particuliere entiteiten voor de rest. Agenten werken op basis van de documenten van de relevante entiteit onder het gezag van die entiteit. De specifieke toewijzingen zijn entiteitsspecifiek en hangen af van de relevante wetgeving en regelingen inzake de schikkingen. Wij erkennen de verdienste van de inzet van het CAC-kader voor milieu-sensoren voor vroegtijdige waarschuwing bij natuurrampen en vervuilingsrisico's, voor agenten voor stroomverdeling en netonderhoud, en voor toepassingen voor de exploratie van hulpbronnen. Wij stellen voor dat in de context van Aotearoa NZ de relevante bevoegdheden voortvloeien uit het bestaande institutionele en verdragsraamwerk, en dat de architectuur de audit- en toewijzingsinfrastructuur biedt waarbinnen die bevoegdheden opereren. Cryptografische herkomst wordt gekoppeld aan milieumetingen, beslissingen over netverdeling en keuzes voor toewijzing van hulpbronnen, met toewijzing aan de verantwoordelijke entiteit (Kroon, iwi of particulier). Federatie-enveloppen vervoeren alleen de goedgekeurde subset van milieugegevens over entiteitsgrenzen heen — vroegtijdige waarschuwingssignalen worden doorgegeven aan alle relevante entiteiten zonder dat centrale aggregatie nodig is. Waar toewijzingen uit verdragsafwikkelingen van toepassing

zijn, beheert de iwi-entiteit haar eigen auditketen onder haar eigen sleutels, onafhankelijk van de systemen van de Kroon. *(Parallellen met CAC-punt 18 “energie en hulpbronnen”.)* [BRONVERMELDINGEN: Resource Management Act 1991 (NZ); relevante wetgeving inzake verdragsafwikkelingen (entiteitsspecifiek, in afwachting van verificatie vóór publicatie van v1); Electricity Industry Act 2010 (NZ); Crown Minerals Act 1991 (NZ).]

Punt 19. In het vervoer zijn soevereiniteitsprincipes van toepassing. Voertuigtelemetrie, verkeersgegevens en infrastructuursensorgegevens zijn soevereine gegevens van exploitanten, overheidsinstanties en wegbeheerders; de coördinatie tussen hen — Waka Kotahi New Zealand Transport Agency, KiwiRail, maritieme autoriteiten, de Civil Aviation Authority, regionale raden en gemeenteraden — is een bilaterale federatie over de relevante institutionele grenzen heen. Wij erkennen de verdienste van de inzet van het CAC-raamwerk voor verkeersveiligheid, noodhulp en intelligente agents voor voertuigcontrole. Wij stellen voor dat de context van Aotearoa NZ, met zijn bestaande bilaterale institutionele regelingen tussen vervoerswijzen, zeer geschikt is voor een gefedereerde aanpak. Federatie-enveloppen specificeren welke telemetrie, verkeersgegevens en infrastructuursensorgegevens worden gedeeld over institutionele grenzen heen (Waka Kotahi ↔ regionale raden ↔ KiwiRail ↔ Civil Aviation Authority), waarbij cryptografische herkomst ervoor zorgt dat forensische reconstructie van elk incident mogelijk is op het niveau van individuele agentbeslissingen. Door leden gestuurde overdraagbaarheid is van toepassing op voertuig- en exploitantniveau — de exploitant kan zonder lock-in om uittreding uit elk platform verzoeken. *(Parallellen met CAC-punt 19 “vervoer”.)* [BRONVERMELDINGEN: Land Transport Act 1998 (NZ); Land Transport Management Act 2003 (NZ); Civil Aviation Act 1990 (NZ); Maritime Transport Act 1994 (NZ); onderzoek naar NZ-werk inzake soevereiniteit van transportgegevens is in behandeling.]

Punt 20. In de landbouw zijn soevereiniteitsprincipes van toepassing. Landbouwgegevens zijn het soevereine dossier van de boer; gegevens over plagen, ziekten, opbrengsten en veestapel mogen bilateraal worden gedeeld met voorlichtingsdiensten, onderzoeksinstellingen of hapū rōpū, indien van toepassing, onder de voorwaarden van de boer. Wij erkennen de verdienste van de toewijding van het CAC-kader aan intelligente agenten voor landbouwdiensten voor technische begeleiding, diagnose van plagen en ziekten, en integratie met slimme landbouwmachines en kassen. Wij stellen voor dat voor Aotearoa NZ — waar soevereiniteit over landbouwgegevens een erkend thema is bij coöperaties voor landbouwgegevens, sectorale organisaties en toenemende betrokkenheid bij de soevereiniteit van de Māori over gegevens in de primaire sector — bilaterale gegevensuitwisseling onder de voorwaarden van de boer zeer geschikt is. Cryptografische herkomst wordt gekoppeld aan landbouwgegevens — sensormetingen, aanbevelingen van agents, behandelingsbeslissingen, opbrengstresultaten. Federatieve enveloppen bevatten alleen de goedgekeurde subset (gegevens over plagen en ziekten aan voorlichtingsdiensten; geaggregeerde opbrengstgegevens aan onderzoeksinstellingen; cultuurcontext-afhankelijke gegevens aan hapū rōpū onder passende tikanga) volgens de voorwaarden van de boer. Dankzij door leden gestuurde overdraagbaarheid kan de boer tussen coöperaties voor landbouwgegevens wisselen zonder zijn historische audittrail te verliezen. *(Parallellen met CAC-punt 20 “landbouwproductie”.)* [BRONVERMELDINGEN: nog op te zoeken voor werk inzake soevereiniteit over landbouwgegevens in Nieuw-Zeeland en regelingen voor het beheer van landbouwgegevens; Te Kāhui Raraunga (kahuiraraunga.io — Māori-model voor gegevensbeheer en Māori-kader voor AI-beheer); Taiuru, K. (20 sep 2025) Kritische analyse van de Te Mana Raraunga-gegevensprincipes, taiuru.co.nz/critical-analysis-mana-raraunga/ waar van toepassing.]

Punt 21. In de financiële dienstverlening zijn soevereiniteitsprincipes van toepassing. Klantgegevens, transactiegegevens en risicosignalen zijn soevereine gegevens van de instelling die ze bewaart, onderworpen aan de prudentiële vereisten van de Reserve Bank

of New Zealand / Te Pūtea Matua, de Privacywet 2020 en de Wet ter bestrijding van witwassen en financiering van terrorisme 2009. AML/CFT-samenwerking is bilateraal via gevestigde kanalen — de New Zealand Financial Intelligence Unit en de internationale FATF-kanalen — en AI-ondersteuning wordt toegeschreven aan en begrensd door deze bestaande regelgevingsafspraken. Wij erkennen de waarde van de toewijding van het CAC-kader aan financiële-risicobeheersingsagenten voor kredietgoedkeuring, transactiemonitoring, accountbeveiliging en antiwitwasmonitoring. Wij stellen voor dat voor Aotearoa NZ het bestaande institutionele en regelgevingskader zeer geschikt is voor op toewijzing gebaseerde controle op het niveau van elke financiële instelling, met bilaterale samenwerking via gevestigde kanalen voor instellingoverschrijdende en internationale coördinatie. Cryptografische herkomst is gekoppeld aan elke transactie, AI-beoordeling en menselijke goedkeuring — achteraf verifieerbaar door AML/CFT-auditors, de Reserve Bank, FATF-inspecteurs en de klant zelf binnen hun respectieve bevoegdheden. Federatieve enveloppen bemiddelen bij instellingsoverschrijdende AML/CFT-samenwerking: alleen het goedgekeurde signaal van verdachte activiteiten wordt doorgestuurd, waarbij de ontvanger gebonden is aan de New Zealand Financial Intelligence Unit of de relevante tegenpartij. Door leden aangestuurde overdraagbaarheid ondersteunt verplichtingen inzake rekeningoverdraagbaarheid: de transactiegeschiedenis van de klant is exporteerbaar naar een andere instelling met intacte herkomst. *(Parallellen met CAC punt 21 “financiële diensten”.)* [BRONVERMELDINGEN: Reserve Bank of New Zealand Act 2021; Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (NZ); Privacy Act 2020 (NZ); FATF-aanbevelingen.]

(III) Dagelijks leven

Punt 22. In eindgebruikersapplicaties zijn soevereiniteitsprimitieven van toepassing. Lid-overdraagbare identificatiecodes vervangen platformspecifieke accounts; coördinatie tussen apparaten wordt bemiddeld door de eigen sleutelbos of identiteitsportemonnee van het lid. Soevereiniteit betekent hier dat de gebruiker de gegevens bewaart — ongeacht of de applicatie is gebouwd door een Aotearoa NZ-leverancier of een internationale leverancier. We erkennen de verdienste van het CAC-raamwerk dat zich inzet voor intelligente agents die internettoepassingen en diensten mogelijk maken op mobiele telefoons, computers, voertuigen, huishoudelijke apparaten, wearables en consumentenrobots. We stellen voor dat voor elke toepassing die werkt met gebruikersgegevens, de architecturale primitieven van attributie en lid-portabiliteit van toepassing zijn, ongeacht de jurisdictie van de leverancier. De operationele primitief is lidgestuurde overdraagbaarheid, geïmplementeerd via W3C Decentralized Identifiers en Verifiable Credentials: de identiteit van de gebruiker wordt bewaard in zijn eigen sleutelbos (of wallet), waarbij de coördinatie tussen apparaten wordt bemiddeld door zijn eigen sleutels. Cryptografische herkomst wordt gekoppeld aan elke actie van een agent met betrekking tot de gegevens van de gebruiker, toeschrijfbaar aan de agent en aan het autorisatiekader van de gebruiker. Federatie-enveloppen bemiddelen alleen bij coördinatie tussen leveranciers wanneer de gebruiker dit toestaat. *(Parallellen met CAC-punt 22 “eindgebruikersapplicaties”.)* [CITATEN: W3C Decentralized Identifiers (DIDs) v1.0; W3C Verifiable Credentials Data Model v1.1; Privacy Act 2020 (NZ), informatieprivacybeginsel 7 (correctie).]

Punt 23. Op het gebied van cultuur en toerisme gelden de basisprincipes van soevereiniteit. Culturele inhoud valt onder de bevoegdheid van de makers ervan; in de context van Aotearoa NZ staan de verplichtingen van de kaitiaki ten aanzien van taonga centraal bij de manier waarop AI-agenten met cultureel materiaal mogen omgaan. Vertaalagenten behouden de bronvermelding en de culturele context; hun output is geen vervanging voor de originele mātauranga, en wat als passend gebruik geldt in te ao Māori-contexten, is aan de tangata whenua om te bepalen. Bezoekersgegevens die door toeristische diensten worden verwerkt, worden behandeld als het soevereine dossier van de bezoeker. Wij erkennen de verdienste van de toewijding van het CAC-kader aan

agenten voor het creëren van culturele inhoud en agenten voor toeristische diensten. Wij stellen voor dat voor Aotearoa NZ — waar mātauranga Māori een taonga is onder de partnerschapsverplichtingen van Te Tiriti, en waar het gepubliceerde werk van dr. Karaitiana Taiuru over de bescherming van mātauranga Māori in AI-trainingsdata, samen met Te Kāhui Raraunga's Māori AI Governance Framework, fundamenteel wetenschappelijk werk vormt — de architecturale primitieven zorgen voor de auditinfrastructuur, en de inhoudelijke bepaling van passend gebruik is voorbehouden aan de houders van de mātauranga. Cryptografische herkomst wordt gekoppeld aan cultureel materiaal: wie heeft het gecreëerd, onder welk gezag, met welk gebruiksbereik. Voor mātauranga bepaalt de tikanga van de houders wat bevoegdheid tot controle in de praktijk betekent; het substraat biedt de auditinfrastructuur zodat schending van toestemming forensisch reconstrueerbaar is, en niet louter contractueel ontkenbaar. Federatie- enveloppen vervoeren alleen de goedgekeurde subset van mātauranga over installatiegrenzen heen, met standaard geen doorsturen — vertaalagenten erven maar kunnen geen nieuwe licenties verlenen. Bezoekersgegevens bevatten de identiteitsverklaring van de bezoeker; lidgestuurde overdraagbaarheid betekent dat de bezoeker bij vertrek zijn toerismegegevensrecord exporteert. *(Parallellen met CAC-punt 23 "cultuur en toerisme".)* [BRONVERMELDINGEN: Taiuru, K. — bescherming van mātauranga Māori in AI-trainingsgegevens (specifieke publicaties in afwachting van verificatie); Te Kāhui Raraunga (kahuiraraunga.io — Māori Data Governance Model en Māori AI Governance Framework); Taiuru, K. (20 sep 2025) Kritische analyse van de Te Mana Raraunga-gegevensprincipes, taiuru.co.nz/critical-analysis-mana-raraunga/; CARE-principes (Carroll et al. 2020); Wai 262 (Waitangi Tribunal-rapport over inheemse flora en fauna en cultureel intellectueel eigendom).]

Punt 24. In commerciële diensten zijn soevereiniteitsprincipes van toepassing. Interacties met klanten leiden tot registraties; beide partijen — exploitant en klant — bewaren kopieën van de herkomst; geschillen worden bilateraal gecoördineerd. Belichaamde agenten in de detailhandel, horeca, ouderenzorg en ondersteuning van mensen met een beperking opereren onder het gezag van de inzetverantwoordelijke en produceren controleerbare registraties van hun handelingen. Wij erkennen de verdiensten van het CAC-kader wat betreft de toewijding aan 24/7 klantenservice, belichaamde intelligente agenten voor begeleiding, schoonmaak, opslag en distributie in commerciële locaties, en belichaamde agenten voor huishoudelijke hulp, ouderenzorg, kinderopvang en ondersteuning van mensen met een beperking. Wij stellen voor dat voor Aotearoa NZ al deze toepassingen opereren binnen bestaande regelgevingskaders voor consumentenbescherming, zorgkwaliteit en diensten voor mensen met een beperking. Beide partijen (exploitant en klant) beschikken over cryptografisch ondertekende herkomstkopieën van elke interactie, zodat geschillen kunnen worden opgelost op basis van een gedeeld, verifieerbaar verslag in plaats van op basis van eenzijdige platformlogboeken. Fysieke assistenten in de detailhandel, horeca, ouderenzorg en ondersteuning van mensen met een beperking werken onder grenshandhaving: beslissingen die afhankelijk zijn van de culturele context of beladen zijn met waarden (overschrijvingen bij medicatietoediening, wijzigingen in zorgplannen, escalaties bij ondersteuning van mensen met een beperking) worden standaard doorgestuurd naar menselijke overweging. De federatie-envelop bemiddelt bij de overdracht van gegevens van het type zorgdossier tussen zorgverleners. *(Parallellen met CAC-punt 24 "commerciële diensten".)* [CITATEN: Consumer Guarantees Act 1993 (NZ); Fair Trading Act 1986 (NZ); Health and Disability Services (Safety) Act 2001 (NZ); New Zealand Disability Strategy.]

(IV) Openbaar welzijn

Punt 25. In het onderwijs zijn soevereiniteitsprincipes van toepassing. Leergegevens zijn het soevereine dossier van de student, met medebeheer wanneer de student minderjarig is; lesmateriaal geproduceerd door agenten wordt toegeschreven; institutionele gegevens — presentielijsten, beoordelingen, kwalificatiegegevens — volgen het bestaande institutionele

bestuur onder de Education and Training Act 2020. Overdraagbaarheid ligt bij de leerling, met passende institutionele regelingen voor de overdracht bij overgangen tussen aanbieders. Wij erkennen de verdienste van de toewijding van het CAC-kader aan het genereren van lesmateriaal, het nakijken van huiswerk, de analyse van leerprogressie, gepersonaliseerde leerplannen en virtuele onderwijsassistenten. Wij stellen voor dat deze mogelijkheden voor Aotearoa NZ functioneren onder de Privacywet 2020 en de Onderwijs- en Opleidingswet 2020, waarbij de soevereiniteit over studentengegevens te allen tijde behouden blijft. Cryptografische herkomstgegevens worden gekoppeld aan elke beoordeling, elk door een agent geproduceerd onderwijsmateriaal, elke toegekende kwalificatie — toeschrijfbaar aan de agent, de begeleidende docent en de instelling. Het soevereine dossier van de leerling is overdraagbaar: bij elke overgang (van school naar school, van school naar universiteit, tussen aanbieders, tussen landen) neemt de leerling zijn volledige dossierbundel met intacte herkomst mee naar de ontvangende instelling. Handhaving van grenzen leidt ertoe dat beslissingen die de beoordeling wijzigen en van invloed zijn op de kwalificaties, standaard worden voorgelegd aan menselijk oordeel. *(Parallellen met CAC-punt 25 “onderwijs en lesgeven”.)* [BRONVERMELDINGEN: Wet op onderwijs en opleiding 2020 (NZ); Privacywet 2020 (NZ); Nieuw-Zeelands leerplan.]

Punt 26. In de gezondheidszorg zijn soevereiniteitsprincipes van toepassing. Patiëntendossiers zijn het soevereine dossier van de patiënt volgens de Health Information Privacy Code 2020 en de beheersstructuren van Te Whatu Ora / Health New Zealand; diagnostische agents produceren geattribueerde uitkomsten; behandelingsaanbevelingen dragen herkomstinformatie; coördinatie tussen zorgverleners vindt plaats via kanalen van de Health Information Standards Organisation (HISO) en interoperabiliteitsafspraken van Te Whatu Ora. Wij erkennen de verdienste van de toewijding van het CAC-raamwerk aan medische beeldvormingsanalyse, redeneringen voor ziektediagnoses, gepersonaliseerde behandelplannen, medicatiebeheer, chirurgische planning en agenten voor het beheer van medische dossiers. Wij stellen voor dat voor Aotearoa NZ deze mogelijkheden functioneren binnen het bestaande governancekader voor gezondheidsinformatie, waarbij de soevereiniteit van de patiënt over gezondheidsdossiers als architectonische basis wordt gehandhaafd. Cryptografische herkomstgegevens worden gekoppeld aan klinische dossiers, AI-diagnostische uitkomsten, behandelingsaanbevelingen en medicatietoediening — waarbij elke invoer herleidbaar is naar de opsteller en onwijzigbaar is voor stille bewerkingen achteraf (correcties zijn medeondertekende wijzigingen, die zelf worden geregistreerd). Federatie-enveloppen bevatten verwijzingen: alleen de goedgekeurde klinische subset wordt verzonden van de verwijzende zorgverlener naar de ontvangende zorgverlener, waarbij de ontvanger standaard gebonden is en niet verder mag doorsturen. Lidgestuurde overdraagbaarheid stelt de patiënt in staat zijn dossierbundel te exporteren naar een andere zorgverlener — publiek, privé of internationaal — zonder toestemming van de oorspronkelijke houder, waarbij de herkomst intact blijft op de bestemming. Handhaving van grenzen leidt klinisch onzekere en waardegeladen beslissingen (levensbeëindiging, betwiste diagnoses, geestelijke gezondheidscompetentie) naar menselijke beraadslaging in plaats van autonome acties van agenten. *(Parallellen met CAC-punt 26 “gezondheidszorg”.)* [BRONVERMELDINGEN: Health Information Privacy Code 2020 (NZ); Pae Ora (Healthy Futures) Act 2022 (NZ); HISO-gegevensstandaarden.]

Punt 27. Op het gebied van werkgelegenheid en arbeid zijn soevereiniteitsprincipes van toepassing. Werkgelegenheidsdossiers, opleidingscertificaten en geschillen zijn soeverein voor de partijen; bemiddeling vindt plaats onder het bestaande bestuur van de Employment Mediation Service; AI-ondersteuning wordt toegeschreven aan en begrensd door de bestaande tripartiete (werknemer / werkgever / staat) structuur van de Nieuw-Zeelandse arbeidswetgeving. Wij erkennen de verdienste van het CAC-kader dat zich inzet voor instanties voor werkgelegenheidsbevordering, opleiding en beoordeling van technisch personeel, arbeidsverhoudingsdiensten, sociale verzekeringen, arbitrage bij arbeidsgeschillen en beheer van achterstallige lonen. Wij stellen voor dat

deze bevoegdheden voor Aotearoa NZ functioneren onder de Employment Relations Act 2000 en het bijbehorende tripartiete kader, waarbij toeschrijving en herkomst overal worden toegepast. Cryptografische herkomst wordt gekoppeld aan arbeidsdossiers, opleidingscertificaten en geschilverslagen — toewijsbaar aan de betrokken partijen. Federatieve enveloppen bemiddelen de overdraagbaarheid van opleidingscertificaten tussen werkgevers zonder verlies van herkomst. Grensafdwinging leidt beslissingen over aanwerving, ontslag, disciplinaire maatregelen en geschillenbemiddeling naar menselijke autoriteit — autonoom optreden van agenten tegen de arbeidsstatus van een individuele werknemer wordt structureel geblokkeerd. *(Parallellen met CAC-punt 27 "human resources".)* [BRONVERMELDINGEN: Employment Relations Act 2000 (NZ); Holidays Act 2003 (NZ); Human Rights Act 1993 (NZ); Nieuw-Zeelands tripartiet kader voor arbeidsverhoudingen.]

Punt 28. In informatiediensten zijn soevereiniteitsprincipes van toepassing. Inhoud wordt toegeschreven aan de makers ervan; aanbevelingsagenten werken op basis van het soevereine profiel van de gebruiker, dat de gebruiker kan inzien, exporteren en overdragen; redactionele beoordeling blijft een menselijke functie. Wanneer AI-agenten inhoud produceren, wordt deze toegeschreven aan de agent en aan de menselijke of organisatorische operator op wiens gezag deze handelde; openbaarmaking van door AI gegenereerde inhoud is de fundamentele architecturale verplichting. Wij erkennen de verdienste van de toezegging van het CAC-kader met betrekking tot intelligente agenten voor de constructie van online-inhoud, gebruikersanalyse, onderwerpplanning, redactionele verwerking, distributie en aanbeveling, inhoudsbeoordeling, opiniebegeleiding, emotionele ondersteuning en realtime vertaling. Wij stellen voor dat voor Aotearoa NZ de toeschrijvingsvereisten van toepassing zijn op al dergelijke toepassingen, waarbij de bestaande omroepnormen en het kader voor schadelijke digitale communicatie de regelgevende context vormen. Cryptografische herkomstgegevens worden aan elk stukje inhoud gekoppeld: identiteit van de auteur, toeschrijving aan AI versus mens, redactionele beoordelingsketen. Federatieve enveloppen bevatten distributiebeslissingen: elk aanbevelingsplatform ontvangt alleen de inhoud die de upstream-installatie heeft ondertekend en waarmee deze heeft ingestemd om te delen, waarbij standaard geen doorgifte plaatsvindt. Door leden gestuurde overdraagbaarheid geeft de gebruiker zijn interactiegeschiedenis en aanbevelingsprofiel in een overdraagbare vorm — hij kan overstappen naar een andere dienst zonder zijn inhoudsgeschiedenis te verliezen. Handhaving van grenzen leidt redactionele beslissingen naar menselijke autoriteit — autonome acties van agenten over wat te versterken of te onderdrukken is structureel geblokkeerd. *(Parallellen met CAC-punt 28 "informatiediensten".)* [BRONVERMELDINGEN: Omroepwet 1989 (NZ); Wet op schadelijke digitale communicatie 2015 (NZ); Privacywet 2020 (NZ); opzoeking naar normen voor AI-inhoudsattributie in behandeling.]

(V) Sociaal bestuur

Punt 29. In het openbaar bestuur gelden soevereiniteitsprincipes. Interacties van burgers met de staat leiden tot documenten die zowel door de burger als de staat worden bewaard; identiteitsgegevens die in het bezit zijn van leden verschuiven in de loop van de tijd naar controle door de leden; agentische ondersteuning bij goedkeuringsprocessen wordt toegeschreven aan en begrensd door beginselen van het bestuursrecht. Overheidsinstanties blijven verantwoording verschuldigd via de Public Service Act 2020, de Official Information Act 1982, de Privacy Act 2020, het Algorithm Charter for Aotearoa New Zealand en de Public Records Act 2005. Wij erkennen de verdienste van de toewijding van het CAC-raamwerk aan agenten voor administratieve goedkeuring, beleidsraadpleging en proactieve dienstverlening. Wij stellen voor dat voor Aotearoa NZ alle dergelijke toepassingen van overheidsinstanties functioneren binnen het bestaande verantwoordingskader, waarbij de architecturale primitieven de auditinfrastructuur bieden die in overeenstemming is met de toezeggingen van het Algoritmehandvest inzake transparantie en partnerschap met de Māori. Cryptografische herkomst is gekoppeld aan elke administratieve handeling: wie

heeft besloten, op grond van welke bevoegdheid, tegen welk burgerdossier, met welke hulp van een instantie. Federatieve enveloppen bemiddelen bij de coördinatie tussen instanties — alleen de goedgekeurde subset van burgerdossiers reist van instantie naar instantie, met audittrail. Door leden aangestuurde overdraagbaarheid geeft invulling aan het informatieprivacybeginsel 6 (toegangsrechten) van de Privacywet en de bewaarplicht van de Wet openbare registers 2005 – de burger kan zijn volledige dossier van interacties met de overheid exporteren onder zijn eigen sleutels. Grenshandhaving leidt beslissingen op basis van administratieve discretionaire bevoegdheid, beslissingen in het kader van verdragsverplichtingen en beslissingen die rechten beïnvloeden naar menselijke autoriteit. *(Parallellen met CAC-punt 29 "openbare bestuursdiensten".)* [BRONVERMELDINGEN: Public Service Act 2020 (NZ); Official Information Act 1982 (NZ); Privacy Act 2020 (NZ); Algorithm Charter for Aotearoa New Zealand (2020); Public Records Act 2005 (NZ).]

Punt 30. In gerechtelijke diensten zijn soevereiniteitsprincipes van toepassing. Gerechtelijke dossiers, bewijsmateriaal en juridische documenten vallen onder bestaande gerechtelijke procedures; AI-ondersteuning wordt vermeld; de bewijsketen is waar van toepassing cryptografisch; toegangscontroles volgen bestaande gerechtelijke regelgeving. Ondersteunende tools voor zelfvertegenwoordigde procespartijen die gebruikmaken van AI maken hun gebruik bekend en leveren een controleerbare herkomst. Wij erkennen de verdienste van de toewijding van het CAC-kader aan end-to-end-ondersteuning bij de behandeling van zaken, het genereren van juridische documenten, juridische publiciteit, juridisch advies en juridische toezichthouders. Wij stellen voor dat voor Aotearoa NZ al dergelijke toepassingen opereren onder de Senior Courts Act 2016, de Evidence Act 2006 en de gevestigde rechtbankregels en praktijknotities die het gebruik van AI in gerechtelijke procedures regelen. Cryptografische herkomst wordt gekoppeld aan elk stuk bewijs dat wordt ingebracht, elk door AI ondersteund concept van een juridisch document, elk zoekresultaat. De bewijsketen is cryptografisch verankerd — vragen over toelaatbaarheid kunnen worden beantwoord op basis van de onderliggende gegevens in plaats van op basis van betwiste platformlogboeken. Lidgestuurde overdraagbaarheid betekent dat de zelfvertegenwoordigde procespartij zijn volledige dossierbundel kan meenemen tussen instanties (tribunaal → rechtbank → beroep) met intacte herkomst. Handhaving van grenzen leidt inhoud met betrekking tot waardeoordelen en discretionaire beslissingen (al dan niet pleiten, al dan niet een schikking accepteren, al dan niet een actie ondernemen die de procespartij benadeelt) naar de menselijke procespartij of diens raadsman — actie van autonome agenten tegen de juridische positie van de procespartij wordt structureel geblokkeerd. *(Parallellen met CAC-punt 30 "gerechtelijke diensten".)* [CITATEN: Senior Courts Act 2016 (NZ); Evidence Act 2006 (NZ); onderzoek naar huidige gerechtelijke richtlijnen inzake AI-gebruik is in behandeling.]

Punt 31. Op het gebied van openbare veiligheid gelden soevereiniteitsbeginselen. Toezicht valt onder bestaande wetgeving — de Privacywet 2020, de Wet op huiszoeking en toezicht 2012 en de Inlichtingen- en veiligheidswet 2017 — en alle AI-agenten die actief zijn in contexten van openbare veiligheid**,** genereren een controleerbare herkomst binnen die kaders. Agenten voor gedragsmonitoring opereren binnen het bereik dat reeds wettelijk is toegestaan onder die wetten. Wij erkennen de verdienste van de toewijding van het CAC- kader aan monitoring- en vroegtijdige waarschuwingsagenten, agenten voor noodhulp en reddingscoördinatie, en toepassingen voor het identificeren van afwijkend gedrag en dynamische preventie. Wij stellen voor, in de context van Aotearoa NZ, dat de architecturale bijdrage van attributie en herkomst erin bestaat om agentische AI in context van openbare veiligheid controleerbaar te maken; of en hoe dergelijke capaciteiten moeten worden ingezet, is een waardenbeslissing voor het relevante wetgevende en beleidsraamwerk, gericht aan het Parlement en de verantwoordelijke ministers, waarbij de architectuur de controle-infrastructuur biedt waarbinnen die beslissingen hanteerbaar worden. Cryptografische herkomst is gekoppeld aan elk surveillancesignaal, elke beslissing over gedragsmonitoring, elke noodhulpactie — waardoor verantwoording achteraf beheersbaar wordt op een manier

die dat bij onbegeleide acties van agenten niet is. Federatieve enveloppen bemiddelen bij de coördinatie van de openbare veiligheid tussen instanties: welke inlichtingen tussen de politie, het Government Communications en noodhulpdiensten wordt bepaald door wat elk heeft goedgekeurd als vrij te geven voor welk specifiek doel. Handhaving van grenzen is hier van cruciaal belang: beslissingen die rechten raken (huiszoeking, arrestatie, toestemming voor surveillance, gebruik van geweld) worden doorgestuurd naar menselijke autoriteiten — de architecturale basis waaronder geen enkele agent autonoom handelt. *(Parallellen met CAC-punt 31 “openbare veiligheid”.)* [BRONVERMELDINGEN: Privacywet 2020 (NZ); Wet op huiszoeking en surveillance 2012 (NZ); Wet op inlichtingen en veiligheid 2017 (NZ); Nieuw-Zeelandse Bill of Rights Act 1990.]

Punt 32. In stedelijk bestuur zijn soevereine basisprincipes van toepassing. Stedelijke gegevens — sensornetwerken, planningsgegevens, bouwvergunningen, operationele infrastructuurgegevens — worden door gemeenteraden bewaard als soevereine documenten; agentsystemen die binnen gemeentelijke functies opereren, worden toegeschreven en zijn verantwoordelijk via de Local Government Act 2002 en gemeentelijke bestuursstructuren. Wij erkennen de verdienste van de toewijding van het CAC- kader aan intelligente agenten voor stadsplanning, stadsbouw en stadsbestuur, onder meer voor slimme bouw, gebouwbeheer en de exploitatie van stedelijke infrastructuur. Wij stellen voor dat voor Aotearoa NZ al dergelijke toepassingen functioneren binnen bestaande verantwoordingsregelingen van de lokale overheid, waarbij de architecturale primitieven de infrastructuur voor controle en toewijzing bieden. Cryptografische herkomst wordt gekoppeld aan elke sensormeting, planningsbeslissing, bouwvergunning en keuze voor infrastructuurbeheer — controleerbaar door inwoners, door Local Government NZ, door de Auditor-General en door opeenvolgende gemeenteraden. Federatieve enveloppen bemiddelen bij de coördinatie tussen gemeenteraden en het delen van gegevens tussen centrale en lokale overheden — alleen de goedgekeurde subset wordt verzonden. Lidgestuurde overdraagbaarheid is van toepassing op gegevens op bewonersniveau: een bewoner kan zijn interacties met de gemeente meenemen wanneer hij van district verandert. Handhaving van grenzen leidt tot beslissingen die verband houden met verdragen en cultureel significant zijn (urupā, wāhi tapu, taonga-beheer) naar de juiste tangata-whenua-beraadslaging in plaats van naar actie door autonome actoren. *(Parallellen met CAC-punt 32 “stedelijk bestuur”.)* [BRONVERMELDINGEN: Local Government Act 2002 (NZ); Building Act 2004 (NZ); Resource Management Act 1991 (NZ).]

Punt 33. Bij aanbestedingen zijn soevereine basisprincipes van toepassing. Aanbestedingsdossiers, evaluaties en contracten zijn soevereine documenten van de aanbestedende dienst; bemiddeling bij aanbestedingen wordt toegewezen en begrensd door de regels voor overheidsopdrachten en het toepasselijke contractenrecht; transparantie wordt gewaarborgd via bestaande, OIA-conforme publicaties. Wij erkennen de verdienste van het streven van het CAC-kader naar end-to-end intelligent beheer van aanbestedings- en biedingsprocessen, waarbij intelligentie wordt toegepast op transacties, diensten en toezicht. Wij stellen voor dat voor Aotearoa NZ de Government Procurement Rules en het bestaande kader voor overheidsopdrachten de juiste context voor verantwoording bieden, waarbij attributie en herkomst overal worden toegepast. Cryptografische herkomst wordt gekoppeld aan elk aanbestedingsdossier, elke evaluatie, elke contractwijziging en elk gunningsbesluit — gepubliceerd onder bestaande OIA-conforme transparantieregelingen met integriteitseigenschappen op substraatniveau. Federatie-enveloppen bemiddelen in de coördinatie van het consortium en de toeleveringsketen die aanbestedingen vereisen, zonder concurrentiegevoelige gegevens buiten het overeengekomen bereik bloot te geven. Grenshandhaving leidt de discretionaire aanbestedingsbeslissingen (gunning, terzijde schuiven, uitzondering) door naar menselijke autoriteit — autonome handelingen van agenten bij een contractgunning worden structureel geblokkeerd. *(Parallellen met CAC-punt 33 “aanbesteding en inschrijving”.)* [BRONVERWIJZINGEN: Regels voor overheidsopdrachten (NZ); Wet op openbare registers 2005 (NZ); Wet op officiële informatie 1982 (NZ).]

§V. Bouwen aan een gefedereerd ecosysteem

Waar het kader van de Cyberspace Administration of China voorziet in een ecosysteem van industriële clusters met nationale koplopers via internationale AI-conferenties, bieden wij een gefedereerd ecosysteem waarin coördinatie plaatsvindt via bilaterale federaties tussen soevereine gelijken en waarbij internationale afstemming verloopt via gevestigde normalisatie-instellingen. De twee volgende subparagrafen — het bevorderen van gefedereerde samenwerking en het versterken van bilaterale promotie — specificeren samen hoe een ecosysteem van soevereine installaties zichzelf in stand houdt en internationaal actief is.

(I) Bevordering van gefedereerde samenwerking

Punt 34. Open source onder permissieve licenties. Referentie-implementaties moeten beschikbaar zijn onder permissieve open-source-licenties. De huidige MDSL-implementaties vormen één set van referenties onder mogelijk meerdere: het Tractatus-framework wordt gedistribueerd onder Apache 2.0 voor code en CC BY 4.0 voor documentatie; de codebases van Village en de community migreren vanaf medio 2026 in fasen naar EUPL-1.2 (European Union Public Licence); toekomstige MDSL- bijdragen zijn bedoeld om, waar mogelijk, onder EUPL-1.2 te vallen, ter afstemming van soevereiniteit met het soevereiniteitswerk van de Europese Unie en ter waarborging van compatibiliteit met bilaterale federatie tussen soevereine installaties in meerdere rechtsgebieden. Wij erkennen de verdienste van het CAC- kader dat zich inzet voor het bevorderen van open-source-innovatie, waaronder binnenlandse open-source-AI-gemeenschappen, compatibiliteit met open-source chips, besturingssystemen en grote modellen, en de betrokkenheid van ondernemingen, universiteiten en onderzoeksinstellingen bij open-source- projecten. Open source onder permissieve licenties is geschikt voor bilaterale federatie: elke soevereine installatie maakt een fork van de upstream, draagt bij via pull-verzoeken en neemt zijn eigen implementatiebeslissingen. *(Parallellen met CAC-punt 34 “bevorder open-source innovatie”.)* [CITATEN: Apache 2.0 (Apache Software Foundation); EUPL-1.2 (European Union Public Licence); CC BY 4.0 (Creative Commons).]

Punt 35. Federatie door publicatie. Waar coördinatie nodig is op het gebied van gemeenschappelijke technologie, interoperabiliteitsnormen, reactie op beveiligingsincidenten of de ontwikkeling van auditkaders, vindt deze plaats via open publicatie en consensus onder de bijdragende installaties. Internationale afstemming verloopt via W3C, IETF, ISO/IEC en soortgelijke gevestigde normalisatie-instellingen. Wij erkennen de verdienste van de inzet van het CAC- kader voor platforms voor samenwerking binnen de sector — waaronder allianties voor ecosystemen van intelligente agenten, laboratoria voor technologische verificatie en gezamenlijke O&O-regelingen — en voor de coördinatie van deelnemers in de toeleveringsketen, zowel stroomopwaarts als stroomafwaarts, bij gemeenschappelijke technologische O&O, normstelling en beoordelings- en certificeringswerkzaamheden. **Dit gebied is werkstroming (iv) van de in §II punt 4 voorgestelde enkele commissie. De commissie zou aanbevelingen in de context van Nieuw-Zeeland ontwikkelen over federatiepatronen en alliantiepatronen voor industriële coördinatie, bijdragen aan het werk van ISO/IEC SC42 aan AI-modellen voor industriële samenwerking, en een bilaterale dialoog aangaan met de auteurs van het CAC-kader over de interactie tussen gefedereerde en op allianties gebaseerde industriële coördinatie.** *(Parallellen met CAC-punt 35 “samenwerkingsplatforms voor de industrie”; de geconsolideerde werkstroom voor de vorming van commissies is van toepassing.)* [BRONVERWIJZINGEN: W3C-procesdocument; IETF Request for Comments-proces; ISO/IEC 42001:2023 managementsystemen.]

(II) Versterking van bilaterale promotie

Punt 36. De goedkeuring is bilateraal. Elke soevereine installatie neemt rechtstreeks contact op met haar tegenpartijen — partnerorganisaties, gelijke instellingen, gefedereerde gelijken. Wij erkennen de waarde van de inzet van het CAC-kader voor kanalen voor applicatiepromotie, waaronder softwarewinkels voor intelligente agents, informatieplatforms voor vraag en aanbod in de industrie, productontwikkeling op maat via aanbestedingen en het “unveil-and-take-the-helm”-uitdagingsmodel, en de ontwikkeling van hardware-systemen en software door ondernemingen voor producten en diensten met intelligente agents. Wij stellen voor, in de context van Aotearoa NZ, dat adoptiekanalen voortkomen uit het bestaande commerciële, maatschappelijke en institutionele landschap; dat overheidsinstanties hun relaties met tegenpartijen opbouwen via gewone directe betrokkenheid, waarbij overheidsopdrachten de regels voor overheidsopdrachten volgen. *(Parallellen met CAC-punt 36 “kanalen voor het promoten van toepassingen”.)* [BRONVERMELDINGEN: Regels voor overheidsopdrachten (NZ); in afwachting van verificatie van eventuele lopende hervormingen van het NZ-aanbestedingsbeleid.]

Punt 37. Proefimplementatie is bilateraal en op bewijs gebaseerd. Soevereine installaties testen de invoering rechtstreeks met bereidwillige gemeenschappen. Bestaande MDSL-implementaties — Village in parochie- en hapū/iwi-contexten; familiegeschiedenis in iwi- en diaspora- contexten; sydigital in kleine-bedrijfscontexten — zijn voorbeelden; specifieke implementatiegegevens (aantallen, startdata, omvang van het huurcontract) moeten worden toegevoegd vóór de publicatie van v1. Wij erkennen de verdienste van het CAC-kader om de opening van toepassingsscenario's voor intelligente agents in sleutelsectoren te stimuleren, met proefprojecten in industriële clusters, sleutelindustrieën en sleutelsectoren die een portfolio van demonstratieprojecten opbouwen. Wij stellen voor dat voor Aotearoa NZ de proefimplementatie bilateraal is tussen de implementerende instanties en hun bereidwillige gemeenschappen. Wanneer overheidsinstanties agentische AI willen testen, doen zij dit in het kader van bestaande processen voor privacy-effectbeoordeling, het Algoritmehandvest voor Aotearoa Nieuw-Zeeland en de toezeggingen van Te Mana Raraunga / Māori Data Sovereignty Network . *(Parallellen met CAC-punt 37 “het bevorderen van de openstelling van belangrijke scenario’s”.)* [BRONVERMELDINGEN: Bewijs van MDSL-implementatie — Village (parochie- en gemeenschapscontexten), familiegeschiedenis (iwi- en diaspora-contexten), sydigital (contexten van kleine bedrijven), specifieke gegevens in afwachting van door de exploitant geverifieerde cijfers vóór publicatie van v1; Algoritmehandvest voor Aotearoa Nieuw-Zeeland (2020); Te Kāhui Raraunga (kahuiraraunga.io — Māori-model voor gegevensbeheer en Māori-kader voor AI-beheer); Taiuru, K. (20 sep 2025) Kritische analyse van de gegevensprincipes van Te Mana Raraunga, taiuru.co.nz/critical-analysis-mana-raraunga/.]

Punt 38. Internationale afstemming via bilaterale federatie. Soevereine installaties in Aotearoa Nieuw-Zeeland sluiten bilaterale federaties met soevereine installaties in andere rechtsgebieden; betrokkenheid bij internationale standaarden vindt plaats via W3C, IETF, ISO/IEC en soortgelijke fora als deelname op basis van gelijkwaardigheid. Wij erkennen de verdienste van de toewijding van het CAC-kader om het wereldwijde ecosysteem actief te cultiveren via internationale platforms zoals de World Artificial Intelligence Conference en de World Internet Conference, de bevordering van de aanpassing van intelligente agents door terminal- en softwarebedrijven, en betrokkenheid bij naleving in het buitenland en aanpassing aan lokale wetten, regelgeving en culturele gewoonten. **Dit gebied is werkstroming (v) van de enkele commissie die wordt voorgesteld in §II punt 4. De commissie zou aanbevelingen in de context van Nieuw-Zeeland ontwikkelen over internationale AI-samenwerking, bijdragen aan het internationale normenwerk van ISO/IEC SC42, en een bilaterale dialoog aangaan met de auteurs van het CAC-kader en met internationale collega's over interoperabiliteit tussen bilaterale-federatie- en platform-projectie-benaderingen van internationale samenwerking.**

We bieden dit aan als een bijdrage aan een internationaal gesprek in een vroeg stadium; bijdragen vanuit vele architecturale tradities en politieke contexten zullen het vakgebied verbeteren. *(Parallellen met CAC-punt 38 “het wereldwijde ecosysteem actief cultiveren”; de geconsolideerde werkstromen voor de vorming van commissies zijn van toepassing.)* [CITATEN: ISO/IEC JTC 1/SC 42; W3C-proces voor internationale normen; onderzoek naar huidige bilaterale AI-overeenkomsten en internationale verbintenissen van Nieuw-Zeeland is in behandeling.]

---

§VI. Waarborging van de invoering

Als voorstander uit het maatschappelijk middenveld coördineert My Digital Sovereignty Ltd de toepassing niet. We noemen hier de instanties waarvan de deelname vereist zou zijn als enig onderdeel van dit raamwerk zou worden toegepast door entiteiten in Aotearoa Nieuw-Zeeland.

Overheidsinstanties waarop dit voorstel betrekking heeft, zijn onder meer het Ministerie van Bedrijfsleven, Innovatie en Werkgelegenheid voor de digitale strategie; het Ministerie van Justitie voor de afstemming van het wettelijk kader; het Bureau van de Privacycommissaris voor de afstemming op de Privacywet 2020; Stats NZ en Te Kāhui Raraunga voor de afstemming op het gebied van gegevenssoevereiniteit (met de kritische analyse van dr. Karaitiana Taiuru van 20 september 2025 als basisreferentie); Te Whatu Ora / Health New Zealand voor het beheer van gezondheidsinformatie; Te Pūtea Matua / Reserve Bank of New Zealand voor de afstemming van het prudentieel toezicht op financiële diensten; Waka Kotahi New Zealand Transport Agency voor vervoer; het Ministerie van Onderwijs voor onderwijs; en de New Zealand Police voor openbare veiligheid. Bij de evaluatie door het maatschappelijk middenveld zouden uiteraard Royal Society Te Apārangi, Internet NZ, NetSafe, het New Zealand AI Forum en academische onderzoekers uit de relevante disciplines betrokken zijn. Inzage door hapū en iwi is essentieel wanneer er sprake is van verplichtingen uit het Verdrag of implicaties voor schikkingen, en de architectuur die dit voorstel specificeert, is bedoeld ter ondersteuning van — en wordt aangeboden voor gebruik in het kader van — het werk op het gebied van Maori-gegevenssoevereiniteit zoals verwoord door Te Kāhui Raraunga (Maori Data Governance Model; Maori AI Governance Framework) en door de gepubliceerde wetenschappelijke publicaties van dr. Karaitiana Taiuru — met inbegrip van zijn kritische analyse van 20 september 2025 waarin wordt toegelicht waarom eerdere kaders ontoereikend zijn voor AI-contexten.

Internationale dialoog met de auteurs van het CAC-kader en met vergelijkbare inheemse netwerken voor gegevenssoevereiniteit — FNIGC in Canada, USIDSN in de Verenigde Staten, Maiam nayri Wingara in Australië, GIDA internationaal — zou beide kanten van het gesprek verrijken.

My Digital Sovereignty Ltd zet zich in voor de architecturale openheid en licentie-openheid van het voorstel: het Tractatus-raamwerk, de Village- en community-codebases en toekomstige MDSL-bijdragen zullen beschikbaar blijven onder permissieve open-source-licenties, en de referentie-implementaties zullen worden ontwikkeld in dialoog met gebruikers. De rest is gericht aan degenen die over de invoering zouden beslissen.

We sluiten af met een expliciete uitnodiging: aan de auteurs van het CAC-raamwerk, aan internationale collega's, aan Nieuw-Zeelandse beleidsmakers en gemeenschapsorganisatoren, en aan iedereen die aan vergelijkbare vraagstukken werkt — opmerkingen over deze v1 zijn welkom via de vaste kanalen voor opmerkingen op agenticgovernance.digital.

Bijlage A. Veelvoorkomende technische bezwaren + reacties

Deze bijlage bevat de meest voorkomende technische bezwaren tegen het Tractatus-raamwerk, met korte structurele reacties. Elke reactie verwijst naar de relevante §0(i)-primitief of een later hoofdstuk. Het raamwerk bevindt zich in de onderzoeksfase; deze reacties vatten de architecturale redenering samen, niet de technische voltooiing.

1. “Hoe kan een LLM iets afdwingen?”

Bezwaar. LLM’s zijn statistische patrooninvullers; vijandige prompts en opkomende mogelijkheden omzeilen de veiligheidsmaatregelen op modelniveau.

Antwoord. Het framework vraagt het model niet om iets af te dwingen. De Tractatus-primitieven zijn runtime-intercepts — code in het hostproces van de agent die beslist of elke voorgestelde actie wordt uitgevoerd, voordat de output van het model de wereld bereikt. De intercept is niet afhankelijk van de compliance- of alignment-training van het model; hij past geconfigureerde beslissingsregels toe op de actiegrenze, dezelfde architecturale vorm als OS-kernel privileged-syscall-interceptie. Zie §0(i) Grenshandhaving.

2. “Hoe zit het met JEPA / alternatieve architecturen?”

Bezwaar. Het framework lijkt uit te gaan van op transformatoren gebaseerde LLM's; architecturale verschuivingen (JEPA, hybride systemen) kunnen het ongeldig maken.

Antwoord. Het raamwerk is substraat-agnostisch. De primitieven werken op acties van de agent, niet op de interne werking van het model — er is geen toegang tot gewichten, aandachtspatronen of redeneringssporen vereist. Een agent op elke architectuur zendt voorgestelde acties uit; de interceptielaag evalueert die acties aan de hand van dezelfde beslissingsklassegrenzen. Zie §0(i) eerste alinea.

3. “Kan de agent de intercept omzeilen?”

Bezwaar. Een agent die bekwaam genoeg is, zou de intercept kunnen modelleren en acties kunnen ontwerpen die deze omzeilen.

Antwoord. De agent heeft niet het privilege om uit te voeren — de interceptie heeft dat wel. Omzeilen vereist ofwel (a) handelen buiten het bereik van de mogelijkheden van de agent, wat door de runtime wordt opgemerkt als een schending van privileges, ofwel (b) volledige privilege-escalatie tegen het hostproces, een kwestie op OS-niveau die op dezelfde manier wordt beveiligd als bij bestandssysteemrechten. Het audittraject (soevereine records, cryptografisch ondertekend) maakt succesvolle omzeilingspogingen forensisch zichtbaar, waardoor 'overlopen als strategie' wordt uitgesloten. Het diepere structurele punt — uitgewerkt in *Architectural Alignment* §3.4 — is het **onderscheid tussen substraat en runtime**: zelfs wanneer een voldoende capabele agent om runtime-onderscheppingen heen redeneert, zijn de substraatmechanismen (cryptografische herkomst, federatie-enveloppen, door leden aangestuurde overdraagbaarheid van records) niet te omzeilen omdat ze in gedistribueerd bezit verkeren, onafhankelijk van de agent. De veiligheid van het substraat vloeit voort uit wiskunde en gedistribueerde replicatie, niet uit de medewerking van de agent. Zie §0(i) Cross-reference validation; §II item 5; *Architectural Alignment* §3.4 substrate-vs-runtime; §7.5 social-layer attack surface (het oppervlak dat het substraat *niet* afsluit).

4. “In hoeverre verschilt dit van de veiligheid van prompt-engineering?”

Bezwaar. Prompt-engineering en RLHF beperken ook de modeloutput. Het raamwerk lijkt qua opzet vergelijkbaar.

Antwoord. Structureel verschillend. Prompt-engineering en RLHF wijzigen de outputverdeling van het model, maar laten dezelfde statistische mechanica intact. De primitieven van het raamwerk worden uitgevoerd vóór het aanroepen van het model (capability-scoping), na de voorgestelde actie (boundary enforcement) of gelijktijdig met het aanroepen (cross-reference validation) — geen enkele is afhankelijk van het feit dat het model de juiste output produceert. Ze zijn afhankelijk van het feit dat de runtime-laag het lidmaatschap van de beslissingsklasse correct identificeert. Zie §0(i) Grenshandhaving en Metacognitieve verificatie.

5. "Wat als de runtime-service zelf wordt misbruikt?"

Bezwaar. Vertrouwen stellen in een runtime-service verplaatst het aanvalsoppervlak in plaats van het te verwijderen.

Antwoord. Het raamwerk beweert niet dat runtime-services onhackbaar zijn. Het beweert dat er bewijzen zijn van afwijkingen en dat die bewijzen de omvang van de schade beperken.

Hoe een inbreuk eruitziet. Ofwel wordt de servicecode misbruikt — een aanvaller onderschept de communicatie om acties buiten het beleid goed te keuren — ofwel wordt de beleidsstatus die de service raadpleegt herschreven — een aanvaller verandert welke beslissingsklassen naar menselijke goedkeuring worden geleid. In beide gevallen is het doel van de aanvaller om een "route naar menselijke" beslissing om te zetten in een "automatisch goedkeuren"-beslissing zonder dat de operator het merkt.

Wat loopt er risico? Beslissingen die het framework anders zou hebben doorgestuurd voor menselijke goedkeuring – waardeoordelen, onomkeerbare bewerkingen, toegang tot gegevens van andere tenants. De omvang van de schade wordt beperkt door wat de intercept al bevoegd was om goed te keuren: het framework verleent toestemming om goed te keuren, geen nieuwe privileges om acties uit te voeren. Een misbruikte intercept kan geen gegevens exfiltreren waar de agent in de eerste plaats nooit toegang toe had; deze kan alleen acties ten onrechte goedkeuren binnen het bestaande bevoegdheidsbereik van de agent.

Oplossingen. Drie eigenschappen komen samen. (i) Elke beslissing van het framework wordt vastgelegd in het soevereine audittraject — cryptografisch ondertekend, alleen-toevoegen, gerepliceerd naar peers — zodat forensische analyse achteraf kan reconstrueren wat er is goedgekeurd, door welke versie van de dienst, en tegen welke beleidsstatus. Het inbreukvenster is beperkt in tijd en omvang. (ii) Validatie via kruisverwijzingen (§0(i)) detecteert afwijkingen tussen waargenomen goedkeuringen en het verklaarde beleid in bijna realtime, waardoor inbreuken aan het licht komen voordat ze de norm worden. (iii) Federatieve replicatie voorkomt dat een aanvaller die één knooppunt controleert, records met terugwerkende kracht kan wissen; om over te lopen is samenspanning met de federatie nodig, niet het compromitteren van een enkele dienst.

Het vertrouwensanker kan falen, maar het falen is begrensd, waarneembaar en forensisch reconstrueerbaar — hetzelfde architecturale patroon als Certificate Transparency voor de TLS PKI: het vertrouwensanker (een Certificate Authority) kan worden gecompromitteerd, maar het auditlogboek van uitgegeven certificaten maakt de compromittering globaal zichtbaar.

De overlevingshouding is gelaagd. De runtime-services van het framework (BoundaryEnforcer, de §0(i)-primitieven) zijn *gericht op de agent*: ze beperken wat de agent kan autoriseren. De sovereign-records-architectuur (Paper A) is *gericht op het substraat*: deze zorgt ervoor dat de records de agent overleven, ongeacht of de agent de poort ontsnapt. Zie *Architectural Alignment* §7.4 (survival posture onafhankelijk van agent-beperking) en §7.5 (het aanvalsoppervlak op de sociale laag dat het substraat niet afsluit — overreding, massaal gecoördineerde identiteitsfraude, gesynthetiseerde toestemming — hier aangeduid als een open grens). Het PKI-handtekeningschema dat ten grondslag ligt aan de auditketen

heeft een kwantumkwetsbaarheidshorizon (10-30 jaar); de NIST-normen voor post-kwantumhandtekeningen zijn in augustus 2024 afgerond en het migratietraject volgt de normen, waarbij vervalsing per record kostbaar is, zelfs op een CRQC, en federatie-/overdraagbaarheidsmechanismen niet afhankelijk zijn van de integriteit van de handtekening. Zie *Paper A* §5.3.

Zie §II punt 5; §0(i) Validatie van kruisverwijzingen.

6. “Wat als waarden veranderen?”

Bezwaar. De grenzen van beslissingsklassen leggen de huidige waarden vast; de waarden van gemeenschappen evolueren, waardoor het raamwerk kwetsbaar wordt.

Antwoord. Beslissingsklassen zijn configuratie, geen architectuur. Het raamwerk biedt het interceptiemechanisme; welke actieklassen naar menselijke goedkeuring worden geleid, is per tenant door de operator bewerkbaar (§III punt 3 — door gebruikers gestuurde governance). Wanneer belanghebbenden binnen een governance-scope onverenigbare grensposities innemen, structureert de pluralistische deliberatie-orkestratie de deliberatie in plaats van een winnaar te kiezen. Het raamwerk is ontworpen om evoluerende waarden te huisvesten, niet om ze te bevriezen. Zie §0(i) Pluralistische deliberatie-orkestratie; §III punt 3.

Licentie en bronvermelding

Voorgestelde bronvermelding: Stroh, J. G. (2026). *Een voorstel van het maatschappelijk middenveld voor soevereine en gefedereerde agentische AI in Aotearoa Nieuw-Zeeland* (v1.2, mei 2026, herzien naar aanleiding van de correspondentie van Ted Howard over v1.1). My Digital Sovereignty Ltd. https://agenticgovernance.digital/papers/aotearoa-nz-agentic-ai-framework-v1.2-may-2026.html

Opmerkingen en correspondentie: Inhoudelijke feedback over specifieke paragrafen is welkom. Vermeld alstublieft paragraafnummers (bijv. §III punt 5) zodat correcties kunnen worden teruggevonden. De auteur beantwoordt persoonlijk; houd rekening met een termijn van één tot twee weken. E-mail: john.stroh@mysovereignty.digital.