



Agentic AI in enterprise-architectuur

Op weg naar een federatie van AI-agents die kennis mobiliseren

Organisaties beschikken over enorme hoeveelheden kennis, maar die kennis zit opgesloten - in documenten, systemen, hoofden van medewerkers en beleidsnotities die zelden worden gelezen. Traditionele digitalisering heeft data ontsloten. De volgende stap is het mobiliseren van *kennis*: het vermogen om informatie te interpreteren, te combineren en om te zetten in onderbouwde beslissingen. **Agentic AI** maakt dit mogelijk.

Agentic AI

AI-agents zijn software die niet alleen informatie verwerkt, maar ook zelfstandig handelt: bronnen raadplegen, informatie interpreteren, adviezen formuleren en acties coördineren. Deze technologie is geen toekomstmuziek - de bouwstenen (grote taalmodellen, integratie-interfaces, cloudplatforms) zijn nu volwassen genoeg voor productie-inzet.

Maar de technologie alleen is niet genoeg. Zonder helder begrippenkader produceren agents schijnbaar correcte maar inhoudelijk onjuiste antwoorden. Zonder betrouwbare kennisbronnen hallucineren ze. Zonder governance-kader opereren ze onbegrensd en oncontroleerbaar.

De kern van deze whitepaper: succesvol inzetten van Agentic AI vereist drie fundamenteën die elke organisatie op orde moet hebben:

1. **Semantische precisie** - begrippen die overal hetzelfde betekenen
2. **Betrouwbare kennisbronnen** - context die herleidbaar en gezaghebbend is
3. **Expliciete governance** - regels die bepalen wat een agent mag en niet mag

Organisaties die deze fundamenteën leggen, bouwen niet zomaar een AI-landschap. Ze bouwen een bestuurbare federatie van digitale expertise die schaalbaar is over afdelingen en organisatiegrenzen heen.

Het probleem: kennis zit opgesloten

Elke organisatie kent het: de informatie is er, maar ze wordt niet benut. Beleidsdocumenten die na goedkeuring in SharePoint verdwijnen. Domeinkennis die alleen in de hoofden van ervaren medewerkers zit. Registraties die technisch ontsloten zijn via API's, maar waarvan de betekenis per afdeling verschilt.

Traditionele digitalisering heeft zich gericht op het delen van *data*. Dat was en is belangrijk. Maar data zonder context is een halffabricaat. Wanneer een medewerker een complexe vraag heeft - "Welke vergunningen zijn nog actief in dit gebied en welke beleidswijzigingen raken die vergunningen?" - dan vereist het antwoord niet alleen data, maar ook interpretatie, combinatie en oordeelsvorming.

Die behoefte wordt urgenter. In de publieke sector lopen vraagstukken steeds vaker over organisatiegrenzen: vergunningverlening, maatschappelijke ondersteuning, gebiedsontwikkeling. In het bedrijfsleven raken supply chains, compliance-trajecten en klantprocessen meerdere afdelingen en partners. In al deze gevallen is data uitwisselen niet genoeg - er moet worden geredeneerd.

Waarom nu?

Drie ontwikkelingen maken dat Agentic AI nu relevant wordt:

1. **Grote taalmodellen zijn productiegereed.** GPT-4, Claude en vergelijkbare modellen begrijpen en genereren natuurlijke taal op een niveau dat bruikbaar is voor professionele toepassingen.

2. Integratie-standaarden ontstaan. Het Model Context Protocol (MCP) standaardiseert hoe AI-agents toegang krijgen tot externe databronnen, tools en kennisbanken.

3. Federatieve data-architecturen rijpen. De Nederlandse overheid en het Europese data spaces-programma bouwen aan de infrastructuur voor organisatieoverstijgend data delen. AI-agents zijn de logische volgende deelnemers in die federatie.

De vraag is niet *of* Agentic AI gaat komen, maar *hoe* organisaties zich erop voorbereiden. Die voorbereiding begint niet bij technologie, maar bij architectuur.

Wat is Agentic AI?

Agentic AI is geen plotselinge doorbraak. De basis - multi-agentsystemen, softwarecomponenten die zelfstandig taken uitvoeren en met elkaar communiceren - bestaat sinds de jaren negentig. Wat nieuw is, is de convergentie van technologieën die agents nu in staat stelt om taken uit te voeren die voorheen menselijke interpretatie vereisten:

- **Grote taalmodellen** die natuurlijke taal begrijpen, waardoor agents niet afhankelijk zijn van starre invoerformaten
- **Integratie-interfaces** (MCP) waarmee agents gestandaardiseerd toegang krijgen tot externe bronnen
- **Cloudplatforms** die de benodigde rekenkracht en schaalbaarheid bieden
- **Kennisbanken en semantische modellen** die agents voorzien van de context om informatie correct te interpreteren

Het resultaat: software die informatie kan verzamelen uit meerdere bronnen, interpreteren aan de hand van begrippenkaders en beleidsregels, en vervolgens een onderbouwd advies formuleren of een actie initiëren.

Implementatie is niet triviaal

De mogelijkheden zijn groot, maar de uitdagingen ook. AI-agents hebben toegang nodig tot databronnen, applicaties, kennisbanken en beleidsdocumentatie. Er moeten kaders worden gesteld voor autorisatie, betrouwbaarheid van bronnen, uitlegbaarheid van beslissingen en architectuurgovernance. Net als bij applicatie-integratie variëren kosten en complexiteit sterk - van een eenvoudige agent die één taak uitvoert tot een ecosysteem van samenwerkende agents.

Zes benaderingen - van eenvoudig tot federatief

Er zijn verschillende manieren om AI-agents in te zetten. Ze variëren van ondersteunend tot autonoom, van intern tot organisatieoverstijgend. In de praktijk worden ze vaak gecombineerd. Het gaat erom bewust te kiezen welke benadering waar passend is.

AI als gereedschap

De meest toegankelijke vorm. AI ondersteunt binnen bestaande applicaties: tekstsamenvatting, classificatie, analyse. De besturing blijft bij de gebruiker.

Voorbeeld: Een medewerker ontvangt een vergunningaanvraag. Het systeem classificeert de aanvraag automatisch, extraheert relevante gegevens en geeft een samenvatting. De medewerker beoordeelt en besluit.

AI in workflows

AI voert taken uit binnen een vooraf gedefinieerde procesketen. De volgorde staat vast, maar AI neemt interpretatie- en analysetaken over.

Voorbeeld: Een toezichthouder ontvangt een melding. De AI verzamelt historische data, analyseert patronen, genereert een risicoprofiel en legt dit voor aan een inspecteur. Na goedkeuring wordt een inspectie ingepland.

De digitale assistent

Een AI-agent die als persoonlijke ondersteuner functioneert. De agent bepaalt zelf welke bronnen hij raadpleegt, maar handelt altijd in opdracht van de gebruiker.

Voorbeeld: Een beleidsmedewerker vraagt: "Wat zijn de gevolgen van dit nieuwe beleid voor lopende vergunningen?" De agent doorzoekt beleidskaders, controleert definities, haalt vergunningdata op en formuleert een onderbouwd antwoord met bronvermelding.

Orchestratie

Een centrale agent stuurt meerdere gespecialiseerde agents aan: een analyse-agent, een compliance-agent, een integratie-agent. De orchestrator coördineert en bewaakt de kwaliteit.

Voorbeeld: Bij een wetswijziging schakelt de orchestrator achtereenvolgens in: een agent die de wettekst analyseert, een agent die de impact op processen beoordeelt, een agent die terminologische consequenties toetst, en een agent die een managementsamenvatting genereert.

Autonome agents met kennisverankering

Agents die zelfstandig opereren, maar stevig verankerd zijn in kennisbronnen. De agent bepaalt zelf welke stappen nodig zijn, maar elke stap wordt getoetst aan gezaghebbende kennis. Dit is de benadering waarbij de kwaliteit van de kennisinfrastructuur het meest bepalend is.

Voorbeeld: Een agent monitort continu wet- en regelgeving, vergelijkt wijzigingen met het bestaande beleidskader, signaleert inconsistenties en genereert een aanpassingsvoorstel met bronverwijzingen. Een medewerker beoordeelt het voorstel.

Federatieve samenwerking

Agents van verschillende organisaties werken samen: ze wisselen niet alleen data uit, maar ook interpretaties, analyses en aanbevelingen. Dit vereist gedeelde afspraken over identiteit, autorisatie, semantiek en governance. We gaan hier in hoofdstuk 5 dieper op in.

Architectuurprincipes

Bij het ontwerpen van een architectuur voor Agentic AI gelden vijf principes. Ze zijn niet abstract - ze hebben directe consequenties voor ontwerpkeuzes.

Transparantie en uitlegbaarheid

Elke beslissing van een agent moet herleidbaar zijn: welke bronnen zijn geraadpleegd, welke redeneerstappen genomen, welke alternatieven overwogen.

Praktisch: als een agent adviseert een vergunning te weigeren, moet herleidbaar zijn welke beleidsdocumenten zijn geraadpleegd, welke begrippen zijn toegepast en welke regels tot de conclusie leiden. Zonder herleidbaarheid is het advies juridisch onbruikbaar.

Scheiding van verantwoordelijkheden

Vier lagen moeten helder gescheiden zijn:

- **Data** - informatiebronnen en registraties
- **Kennis** - context en betekenis (begrippenkaders, beleidsdocumenten)
- **Logica** - AI-modellen en redeneerstappen
- **Governance** - regels, mandaten en beperkingen

Wanneer een agent zelf bepaalt wat een begrip betekent in plaats van een gezaghebbend begrippenkader te raadplegen, ontstaan onbeheersbare systemen.

Semantische consistentie

Het begrip *inkomen* bij de Belastingdienst is niet hetzelfde als *inkomen* bij een woningcorporatie. Zonder gedeeld semantisch fundament produceren agents schijnbaar correcte maar inhoudelijk onjuiste resultaten. Elke agent die domeinoverstijgend opereert, moet begrippen valideren tegen een gezaghebbend begrippenkader.

Governance en controle

Agents mogen niet onbeperkt opereren. Regels voor toegang, gebruik en actie moeten niet impliciet in code zitten, maar expliciet vastliggen in de architectuur. Per agent moet vastliggen: op welk domein mag hij opereren, welke bronnen mag hij raadplegen, welke acties mag hij uitvoeren.

Menselijke controle

Hoe autonoom agents ook worden, voor belangrijke beslissingen moet altijd een *human-in-the-loop* mogelijk zijn. Definieer per type beslissing: mag de agent autonoom handelen, moet hij een advies voorleggen, of mag hij alleen informatie verzamelen? Leg deze escalatieniveaus vast in de architectuur.

Van interne AI naar federatieve samenwerking

De eerste vijf benaderingen spelen zich af binnen één organisatie. Maar veel vraagstukken zijn organisatieoverstijgend. Vergunningverlening raakt meerdere overheidslagen. Zorgketens verbinden zorginstellingen, gemeenten en zorgverzekeraars. Supply chains omvatten tientallen partijen.

In Nederland is veel geïnvesteerd in federatieve data-architecturen: data vindbaar en bruikbaar bij de bron, zonder centraal te kopiëren. De referentie-architectuur voor gegevensruimtes maakt onderscheid tussen een *data plane* (waar data zich bevindt) en een *control plane* (waar afspraken over identiteit, autorisatie en vertrouwen worden geregeld).

De volgende sprong: wat als niet alleen systemen en datasets deelnemen, maar ook AI-agents?

Een klassieke service voert een vast contract uit: request erin, response eruit. Een AI-agent werkt anders. Die interpreteert een vraag, bepaalt zelf welke bronnen relevant zijn, redeneert en formuleert een antwoord dat niet vooraf bepaald is. Wanneer zulke agents samenwerken over organisatiegrenzen, ontstaat een nieuw type integratie.

Een nieuw integratieportfolio

Naast de bekende integratievormen ontstaan drie nieuwe:

Type	Beschrijving	Status
System-to-system	Klassieke applicatie-integratie	Bekend terrein
System-to-data	Ontsluiten van databronnen via API's en data spaces	Bekend terrein
Agent-to-tool	Agent krijgt toegang tot externe hulpmiddelen via MCP	Nieuw
Agent-to-agent	Agents werken samen, verdelen taken, delen context	Nieuw
Agent-to-governance	Agents toetsen hun handelen aan vastgelegde regels	Nieuw

De laatste drie vragen om een nieuw architectuurraster. Zodra agents context delen en autonoom redeneren, worden vragen over vertrouwen, verantwoording en semantische consistentie fundamenteeler dan bij traditionele data-uitwisseling.

De denkfout: federatie is geen technisch integratievraagstuk

Het draait om semantiek, governance en vertrouwen. Welke begrippen worden gedeeld en wat betekenen ze? Welke bronnen zijn gezaghebbend? Wie is verantwoordelijk als een agent een onjuist advies geeft? Deze vragen moeten beantwoord zijn *vóórdat* agents over organisatiegrenzen samenwerken.

De cognition plane - een nieuwe architectuurlaag

De referentie-architectuur voor gegevensruimtes kent twee lagen. Voor AI-agents is een derde nodig.

Laag	Bevat	Governance-vraag
Data plane	Datasets, API's, events, documenten	Wie mag welke data opvragen en onder welke voorwaarden?
Control plane	Identiteit, autorisatie, contracten, logging	Hoe borgen we vertrouwen en naleving?
Cognition plane	Agents, doelen, redeneerpatronen, escalatieregels	Hoe borgen we dat redenering betrouwbaar, herleidbaar en begrensd is?

De cognition plane is geen uitbreiding van de control plane. Het is een wezenlijk nieuwe laag. Agents voeren niet alleen beleid uit - ze produceren nieuwe semantische samenstellingen: analyses, adviezen en interpretaties die niet vooraf gedefinieerd zijn.

Waarom is dat onderscheid belangrijk? Omdat governance van redenering andere mechanismen vereist dan governance van datastromen. Bij data gaat het om toegang en kwaliteit. Bij agents gaat het om mandaten, redeneergrenzen, bronvalidatie en verantwoording van conclusies die niet deterministisch zijn.

Drie fundamenteën voor de cognition plane

In de cognition plane zijn drie componenten onmisbaar:

1. Semantische precisie - agents moeten begrippen eenduidig interpreteren. Zonder gezaghebbend begrippenkader produceren ze antwoorden die er correct uitzien maar inhoudelijk onjuist zijn.

2. Betrouwbare context - agents moeten hun antwoorden gronden in gezaghebbende bronnen, niet in algemene trainingsdata. Elk advies moet herleidbaar zijn tot concrete passages in beleidskaders, richtlijnen of registraties.

3. Expliciete governance - per agent moet vastliggen: welke doelen, welke mandaten, welke bronnen, welke grenzen. Dit moet niet impliciet in code zitten maar expliciet in de architectuur.

Zonder deze drie fundamenteën ontstaat agentgedrag dat technisch indrukwekkend kan zijn, maar institutioneel onbetrouwbaar.

Hoe ArchiXL-producten hierin passen

De drie fundamenteën van de cognition plane vragen om concrete tooling. ArchiXL biedt drie producten die hier elk een specifieke rol vervullen.

BegrippenXL - semantisch fundament

BegrippenXL is een platform voor het beheren van begrippenkaders. Organisaties leggen vast wat termen precies betekenen, hoe ze zich verhouden en welke definities gezaghebbend zijn. Gebaseerd op de NL-SBB standaard van Geonovum.

Rol in Agentic AI: BegrippenXL fungeert als semantisch kompas. Bij elke stap in het redeneerproces valideert de agent of hij begrippen gebruikt conform de gezaghebbende definities. Een agent die *huishouden*, *vergunning* of *maatwerkvoorziening* verkeerd interpreteert, levert onbetrouwbare resultaten - ongeacht hoe goed het taalmodel is.

WikiXL - kennisbank en grounding-laag

WikiXL is een platform voor het structureren en ontsluiten van organisatiekennis: beleidskaders, werkprocessen, domeinkennis en richtlijnen. Vindbaar, versioneerbaar en herleidbaar.

Rol in Agentic AI: WikiXL is de grounding-laag. Wanneer een agent een advies genereert, moet dat advies herleidbaar zijn tot concrete passages in het beleidskader - niet tot het algemene trainingsgeheugen van een taalmodel. WikiXL maakt die herleidbaarheid mogelijk via MCP-integratie.

ArchiMedes - de bestuurbare architectuurkaart

ArchiMedes is het enterprise-architectuurplatform van ArchiXL. Organisaties leggen er hun applicatielandschap, informatiestromen, processen en governance-afspraken vast.

Rol in Agentic AI: ArchiMedes wordt de plek waar de spelregels voor agentgedrag worden vastgelegd: welke agent mag op welk domein opereren, welke bronnen zijn gezaghebbend, welke interfaces bestaan, welke policies gelden. Niet alleen leesbaar voor architecten, maar ook raadpleegbaar voor agents.

Interactie in de praktijk

Een overheidsmedewerker stelt de vraag: *"Welke vergunningen zijn actief in dit gebied en welke beleidswijzigingen raken die?"*

1. Een **orchestrator** interpreteert de intentie en bepaalt welke agents nodig zijn
2. Een **semantische agent** raadpleegt BegrippenXL voor eenduidige begrippen
3. Een **data-agent** haalt vergunninggegevens op uit bronregistraties
4. Een **kennisagent** doorzoekt WikiXL voor relevante beleidskaders
5. Een **compliance-agent** toetst via ArchiMedes of de bronnen gezaghebbend zijn en de agent gemachtigd is
6. De orchestrator combineert tot een onderbouwd antwoord met bronvermelding

Het verschil met een gewone zoekmachine: elk antwoord is herleidbaar tot begrippen, bronnen, beleid en architectuurregels.

Implementatie in vijf stappen

Stap 1: Kennisinfrastuur op orde

Voordat je agents inzet, moet het fundament staan:

- **Begrippenkaders formaliseren** - begin met begrippen die het meest worden gedeeld tussen afdelingen
- **Kennis structureren** - beleidsdocumenten en richtlijnen vindbaar en gestructureerd beschikbaar maken
- **Architectuur actualiseren** - applicatielandschap, informatiestromen en governance-afspraken vastleggen

Stap 2: Afgebakende use case

Kies een use case die complex genoeg is om waarde te demonstreren, maar beheersbaar genoeg om mee te starten:

- Intern kennisportaal met AI-assistent die beleidsvragen beantwoordt
- Automatische classificatie en routing van meldingen
- Impact-analyse bij wijzigingen in wet- en regelgeving

Stap 3: Governance-kader definiëren

Leg vast vóór implementatie:

- Welke bronnen mag de agent raadplegen?

- Welke acties mag hij uitvoeren en welke vereisen menselijke goedkeuring?
- Hoe worden antwoorden herleidbaar gemaakt?
- Wie is verantwoordelijk bij onjuiste uitkomsten?

Stap 4: Iteratief bouwen en testen

Begin met een agent die informatie ophaalt en samenvat. Breid geleidelijk uit naar interpretatie, advies en gecoördineerde actie. Test per iteratie: zijn antwoorden correct en herleidbaar? Worden begrippen consistent gebruikt? Handelt de agent binnen mandaten?

Stap 5: Opschalen

Pas wanneer architectuur en governance bewezen zijn:

- Meerdere samenwerkende agents (orchestratie)
- Organisatieoverstijgende agents (federatief)
- Integratie met externe data spaces

De strategische les

De conclusie is scherp:

- Een federatief stelsel zonder semantiek blijft een logistiek netwerk.
- Een federatief stelsel met AI-agents zonder governance wordt een risico.
- Een federatief stelsel van AI-agents, gevoed door begrippen, kennis en architectuur, wordt een intelligent ecosysteem.

Begin niet met de vraag *welke AI-tool zullen we invoeren*. Begin met drie fundamentele vragen:

- 1. Welke begrippen moeten overal hetzelfde betekenen?**
- 2. Welke kennis mag als gezaghebbende context dienen?**
- 3. Welke architectuurregels begrenzen autonoom agentgedrag?**

Wie die drie vragen beantwoordt, bouwt een bestuurbare federatie van digitale expertise. En dan wordt de toekomst concreet:

- **BegrippenXL** wordt het semantische kompas
- **WikiXL** wordt het gedeelde geheugen
- **ArchiMedes** wordt de bestuurbare landkaart

Dat is de volgende volwassenheidsstap van enterprise-architectuur.

Over ArchiXL

ArchiXL is een onafhankelijk adviesbureau, gespecialiseerd in enterprise- en informatie-architectuur. Wij adviseren organisaties bij het operationaliseren van hun strategie. De naam ArchiXL is een samenvoeging van "Architectuur" en "XL", waarbij XL staat voor "excelleren". Wij helpen organisaties om hun doelen te bereiken waardoor zij kunnen excelleren. Onderscheidend daarbij is onze pragmatische en doelgerichte werkwijze. Dat zorgt dat we sterk gericht zijn op het leveren van toegevoegde waarde, passend bij de context van de organisatie. Als specialist op het gebied van architectuur kennen we alle relevante methoden en technieken en weten we als geen ander wat de valkuilen zijn. Onze medewerkers onderscheiden zich door hun communicatieve vaardigheden, resultaatgerichtheid, en hun abstractie- en inlevingsvermogen.

Het is onze passie om de doelmatigheid en effectiviteit van veranderingen en de wijze waarop architectuur en kennis daarbij worden toegepast, te verbeteren. Wij denken dat mensen en hun kennis daarin de sleutelfactoren zijn en ondersteunen dat met onze producten ArchiMedes, BegrippenXL en WikiXL.

Onze principes

- Standaard methode – onze aanpak is gebaseerd op standaard methoden en technieken zoals ArchiMate en TOGAF, en daarmee op uitgebreide kennis en ervaring van anderen.
- Hergebruik – organisaties lijken in veel opzichten op elkaar en hergebruik van kennis en architecturen is daarom verstandig.
- Iteratief werken – het is belangrijk om snel antwoord te geven op vragen vanuit de organisatie; dit hoeft niet altijd een volledig antwoord te zijn.
- Concrete en bruikbare resultaten – architectuurproducten moeten direct bruikbaar zijn en waarde opleveren voor de organisatie.
- Samenwerking – veranderen doe je samen, daarmee bundel je ook de kennis en denkvermogen en ontstaat draagvlak voor de verandering.
- "Just enough" architectuur – architectuurdocumenten moeten bijdragen aan de doelstellingen en niet meer beschrijven dan noodzakelijk.
- Mobiliseren kennis – architecten moeten zich vooral richten op het verzamelen, analyseren, genereren en verspreiden van kennis.

Meer weten?

telefoon: 030-3074310

e-mail: info@archixl.nl

website: <http://www.archixl.nl>