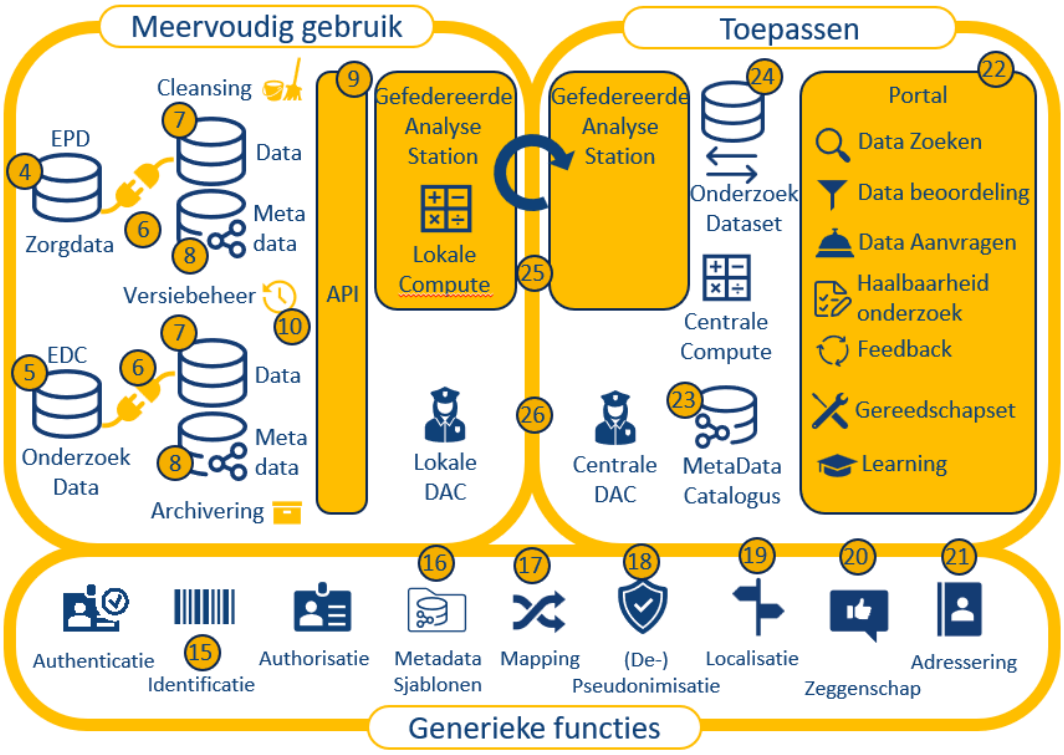
Strategisch perspectief

Verhaallijn AI dataplatform (AIDA)

Secure Processing Environments voor secundair gebruik van gezondheidsdata

Versie 4 van de Health-RI wiki beschrijft de gezondheidsdata-infrastructuur voor onderzoek, beleid en innovatie. Deze infrastructuur is specifiek gericht op secundair gebruik, en is een verbijzondering van de algemene gezamenlijk gezondheidsdata architectuurmodel. Binnen deze architectuur zijn reeds twee soorten van Secure Processing Environments benoemd, namelijk veilige verwerkingsomgevingen) en gefedereerde verwerkingsomgevingen.



Figuur 1: Conceptuele architectuur voor secundair gebruik

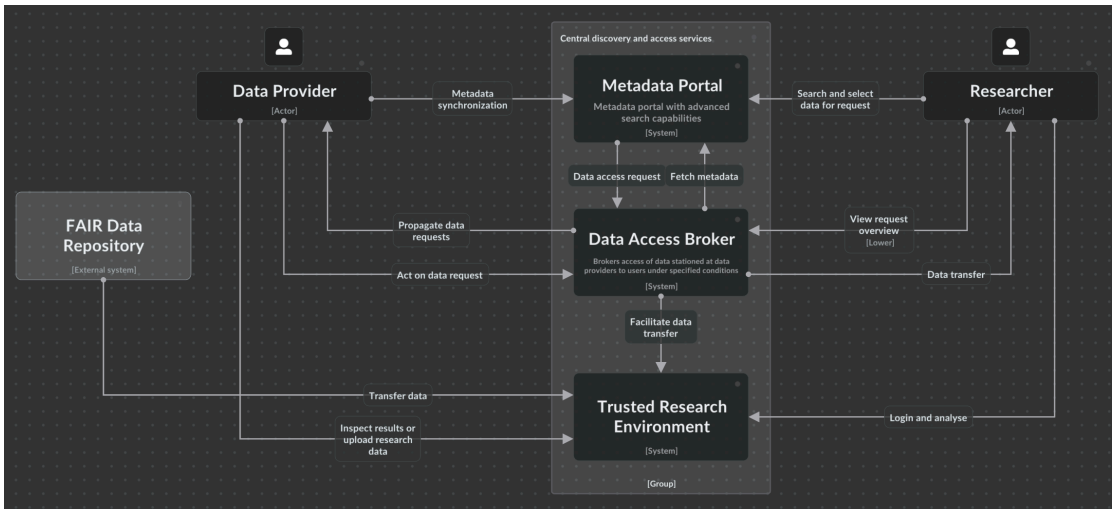
De basis gedachte achter AIDA is dat er *verschillende soorten van* ***secure processing environments*** zullen zijn. Als start voor de discussie introduceren we een derde type, de hybride Secure Processing Environment (H-SPE). In dit document hanteren we de namen van deze drie typen om expliciet onderscheid te maken; we zullen spreken van SPEs in het algemeen als we alle drie de soorten bedoelen. We geven een korte schets en voorbeeld van elk type.

Tabel 1: Drie soorten van Secure Processing Environments die binnen de scope van AI-DA vallen.

Gecentraliseerde SPE	• vaak benoemd als Trusted Research Environment • veel bestaande voorbeelden, zie o.a. EOSC-ENTRUST • machine learning op tabulaire data mogelijk • *statistical disclosure control* op output
Federated SPEs	• decentrale benadering cf. personal health train • oorspronkelijk bedoelt voor machine learning • kan ook gebruikt worden voor statistische analyse • moeilijker om mee te werken
Hybride SPE (H-SPE)	• Combinatie van bovenstaande technieken • Nodig om gebruik te maken centrale rekencapaciteit • Gedachte om gebruiksgemak te verbeteren

TRE: SURF Secure Analysis Environment (SANE)

SURF Secure ANalysis Environment (SANE) is een virtuele, volledig afgeschermde omgeving waarop met vooraf goedgekeurde analyse software draait en toegang tot sensitive data wordt gegeven (Figuur 2). In onderstaand overzicht is SANE gepositioneerd als TRE, waarmee de data aanbieder controle houdt over de data die ter beschikking wordt gesteld en waarmee de data consumer op een makkelijke manier toegang krijgt. SANE biedt functionaliteiten op het gebied van *Research Analytics*, *Secure Data Zone* en *Data Discovery*. Meer details staan in de blauwdruk van EOSC-ENTRUST.



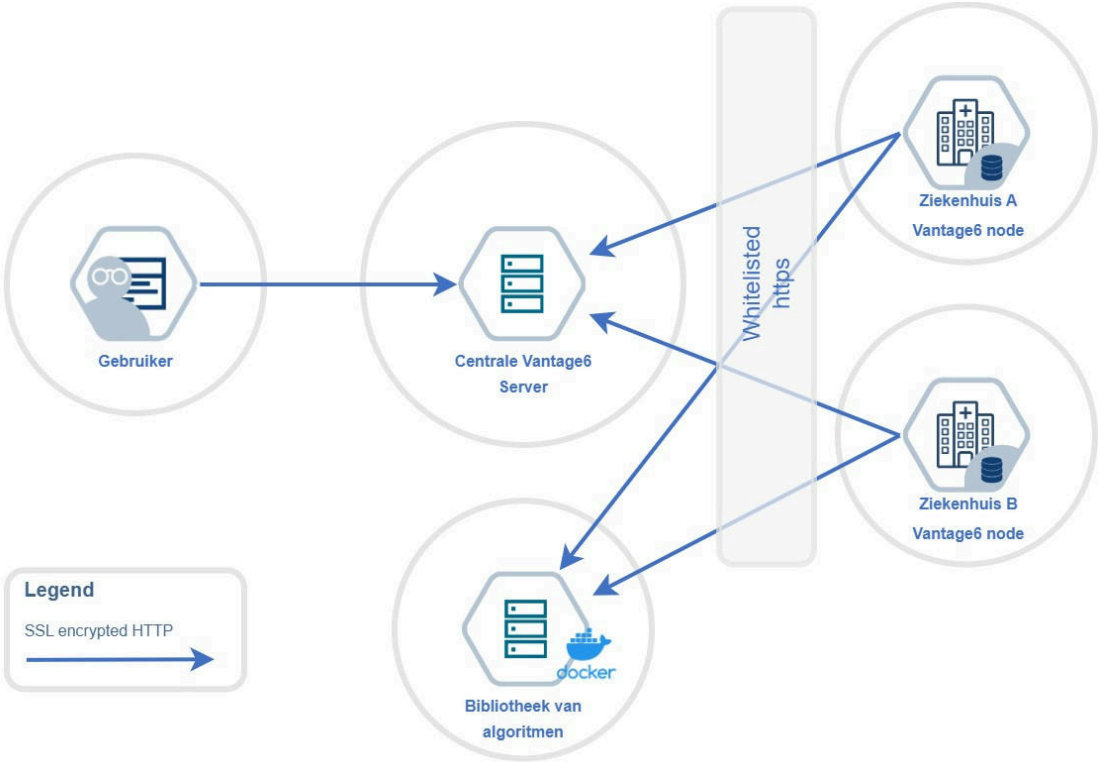
Figuur 2: Positionering van SANE binnen een generieke data space architectuur.

Belangrijk kenmerk van SANE en andere TREs is dat de data fysiek naar de *Secure Data Zone* wordt gekopieerd. Naast het veilig aanbieden van data (als data houder), is dit ook het mechanisme waarmee data gebruikers hun eigen data mee kunnen nemen naar de TRE, om daarbinnen te koppelen aan andere data. Dit gebeurd vaak met gebruik van pseudonimisering. De CBS microdata omgeving werkt op een vergelijkbare manier.

Binnen de blauwdruk van EOSC-ENTRUST wordt gesproken over *Federation Services* tussen verschillende TREs. Daarbij gaat het om data federation: data wordt (tijdelijk) van de ene naar de andere TRE gekopieerd zodat het daar in combinatie verwerkt kan worden. Data federation als mechanisme is anders dan federated learning: daarbij worden de berekeningen decentraal uitgevoerd en alleen de resultaten centraal gedeeld (zie hieronder). Federated learning is met name nuttig voor horizontaal gepartitioneerde data. Voor verticaal gepartitioneerde data, is data federation zoals beschreven door EOSC-ENTRUST meer geschikt.

FLN: PLUGIN/vantage6

Federated learning (FL) als concept staat ook wel bekend als de Personal Health Train (PHT). De term FL wordt vooral gebruikt om naar het technische concept te verwijzen, terwijl PHT verder gaat in het definiëren van afspraken rondom het gebruik van FL. Het basis principe is dat bij FL de gegevens op afzonderlijke 'data stations' verschillende apparaten blijven die participeren in het FLN. Om deze data te gebruiken voor machine learning, wordt bij elk data station het algoritme lokaal c.q. afzonderlijk getraind. Vervolgens worden alleen de resultaten van het algoritme - bijvoorbeeld geaggregeerde statistieken of de modelparameters van het neurale netwerk - gedeeld met een centrale server. Deze server combineert de resultaten van afzonderlijke modellen tot één model, welke vervolgens met alle deelnemers van het FLN gedeeld wordt.



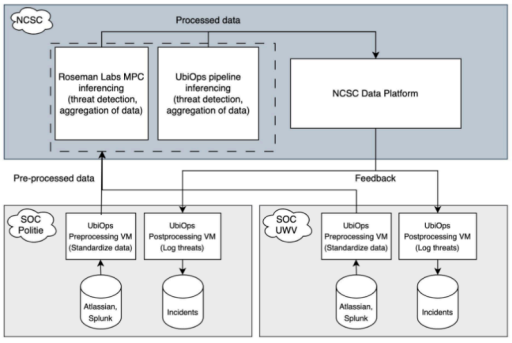
Figuur 3: Overzicht van vantage6 infrastructuur zoals in PLUGIN is gerealiseerd.

Het PLUGIN project heeft een FLN van tientallen ziekenhuizen gerealiseerd, waarbij gebruik wordt gemaakt vantage6 als platform. Belangrijkste kenmerken van deze opzet zijn:

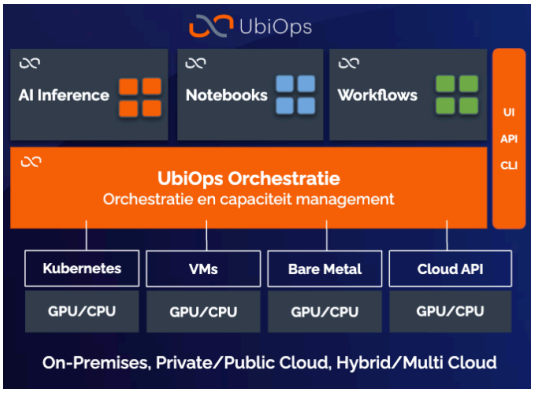
- Sterke nadruk op veiligheid en privacy, door gebruik van beveiligde containers en virtual private networks in de basis infrastructuur
- Ontzorgen van deelnemende ziekenhuizen, waarbij gebruik wordt gemaakt van een generieke Linux server in het domain van het ziekenhuis dat als basis dient om de opslag en rekenkracht voor de FLN te realiseren. Afhankelijk of een ziekenhuis mee doet als trainingsziekenhuis of alleen als gebruiker dient een zwaardere resp. lichtere Linux server te worden geconfigureerd
- Voor elk project wordt de berekening c.q. machine learning expliciet 'verpakt' in een Docker container, zijnde de berekening die daadwerkelijk wordt uitgevoerd.
- De generieke Linux server wordt ook gebruikt om dashboard, informatieproducten etc. te hosten binnen het IT domein van het ziekenhuis

Het gebruik van een standaard data model (op de data stations) is een belangrijke randvoorwaarde om FL te kunnen doen. Naast het gebruik van vantage6 als kerntechnologie, heeft PLUGIN ervoor gekozen om FHIR als data standaard te gebruiken. Hiertoe is een FHIR profiel in ontwikkeling die aansluit op de bestaande ZIBS2020 bouwstenen. Meer achtergrond over de keuze voor FHIR is te lezen in dit artikel. Andere voorbeelden van FLN platform zijn hier te vinden.

H-SPE: UbiOps en Roseman Labs



Figuur 4: Hybride samenwerking tusssen SOCs



Figuur 5: UbiOps orchestratielaag

De hybride SPE is een nieuwe oplossingsrichting die we willen verkennen (en realiseren) in AIDA. Er zijn veel minder concrete voorbeelden van een dergelijke opzet. UbiOps en Roseman Labs hebben een oplossing die er het dichts bij in de buurt komt (Figuur 4). In analogie met data spaces, gaat het hier om het verbinden van verschillende Security Operating Centra (SOC) in de beveiligingsketen (NCSC, politie, UWV etc.) In een H-SPE kunnen *compute* (rekenkracht) en *storage* (opslag) zowel lokaal als centraal worden uitgevoerd. In deze architectuur worden bijvoorbeeld pre-processing van data decentraal uitgevoerd in de SOCs in de onderste laag van Figuur 4. De resultaten van deze pre-processing gaan naar het centrale platform, in dit geval de NCSC. Daar kunnen vervolgens ook weer (vervolg-)berekeningen worden uitgevoerd, op de *storage* en *compute* die beschikbaar zijn in de omgeving van de NCSC.

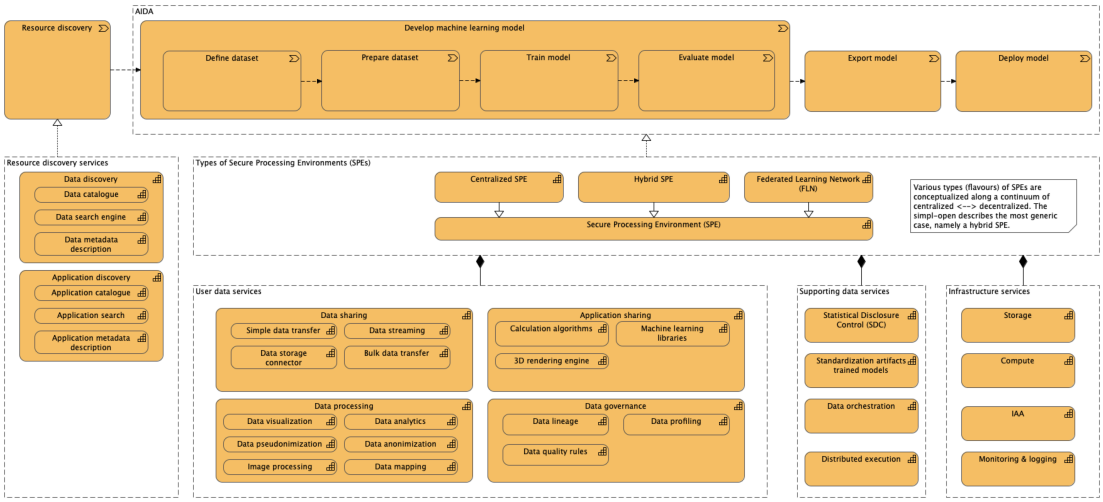
Deze opzet bij de NCSC is mogelijk gemaakt door UbiOps, een platform leverancier die de orkestratielaag biedt waarmee alle *storage* en *compute* centraal wordt beheerd (Figuur 5). Een belangrijk ontwerpprincipe van deze orkestratielaag is dat het verschillende soort fysieke infrastructuur kan managen, variërend van *bare metal* servers, Kubernetes cluster, virtuele machines, public cloud infrastructuur etc.

Een ander onderscheidende kenmerk van de opzet bij NCSC is dat de centrale dataverwerking ook onder encryptie uitgevoerd kan worden via het Roseman Labs MPC (Multiparty Computation). Door berekeningen *in-the-blind* uit te voeren, zijn de data extra beschermd.

Alhoewel er nog weinig voorbeelden zijn van operationele H-SPEs, is deze opzet in lijn met de recent gepubliceerde Simpl-Open architectuur. Kenmerken van het NCSC platform zien we daarin terugkomen als ontwerpprincipes, waaronder:

- Het gebruik van *agents* als mechanisme voor het orkestreren van allerlei *compute* en *storage* binnen een data space en tussen een data space
- Mogelijkheid om over verschillende fysieke locaties een data space op te zetten
- Sterke nadruk op Identificatie, Authenticatie en Autorisatie (IAA) functies, waarvoor standaarden gebruikt moeten worden
  - Tier 1: IAA van gebruikers
  - Tier 2: IAA voor machine-to-machine orkestratie
- Naast gebruik van catalogi voor data en applicaties wordt ook het gebruik van een infrastructuur voorgeschreven, zodat daarmee inzichtelijk is welke *compute* en *storage* beschikbaar is binnen het netwerk.

Praatplaat AIDA



Figuur 6: Praatplaat (strategy view)

Eerste schot voor de boeg. Deze praatplaat gaan we bespreken om de scope en omvang van AIDA te bepalen, en wanneer die voldoende helder is gaan we het detailleren en uitwerken. In de rest van dit hoofdstuk beschrijven we:

- Relevante blauwdrukken en referentiearchitecturen

- Verschillende voorbeelden van AIDA-achtige platformen die op dit moment al in ontwikkeling zijn c.q. draaien, als inspiratie voor de discussies

Lijst van relevante projecten en componenten

- https://molgenis.org/ : analyse platform bioinformatics
- https://www.openplanet.cloud/data-platform : analyuse
- https://www.yivi.app/ : Identity mgnt
- https://checkmk.com/ : OSS operations & observability

Bibliografie