Verslag werkgroep Toegang

Aanwezig: Frits Bouma (DUO), Edwin Verwoerd (KBb-E), Freek Nabuurs (Cito), Peter Clijsters (SURF), Bram Gaakeer (OCW, voorzitter), Erwin Reinhoud (Kennisnet, Bureau Edustandaard), Joris Dirks (Studielink), Paul de Wit (saMBO-ICT/MBO Raad), Dirk Linden (Kennisnet), Brian Dommisse (Kennisnet, PO/VO-raad)

Afwezig: Tom van Veen (SURF)

Datum
17 februari 2022

Agenda

1. Opening en mededelingen
2. Vaststellen verslag december 2021 en actiepunten
3. Modellen en deliverables
4. Toelichting MORA

1. Opening en mededelingen

Agenda wordt zonder wijzigingen vastgesteld.

Er wordt gemeld dat Forum Standaardisatie een openbare consultatie is gestart voor het NL GOV OpenID Connect profiel. De einddatum voor de consultatie is 25-02-2022. Op basis hiervan wordt vastgesteld of deze geschikt is om te verplichten (ptolu) voor de overheid.

SURF is bij de expertbijeenkomst betrokken. Peter gaat ervoor zorgen dat we een volgende keer een toelichting krijgen, wat zijn de kernpunten van het profiel en is SURFconext compliant of zijn er plannen dit te worden (actiepunt#).

2. Vaststellen verslag 27 januari en actiepunten

2.1. Verslag

Geen opmerkingen

2.2. Actiepunten

Actiepunt #5 Voorstel om aanpak uit te breiden met autorisatie rollen en het proxy model (Erwin)

- Geen wijzigingen

Actiepunt #8: Kaders voor thema toegang ontwikkelen tbv ROSA scan. (Bram/Erwin)

- Geen wijzigingen

Actiepunt #19: Nadat kaders zijn opgesteld gaan we nog eens door attributentabel, welke tributen zijn wanneer nodig

- Wordt na principes document geëvalueerd.

Actiepunt #20: Aan de attributentabel ook de doelen (Audit)Logging en Support toevoegen

- Wordt met #19 meegenomen

Actiepunt #21: Check eduID op de generieke functies van Principes en ontwerpeisen

- Geen wijzigingen

Actiepunt #22: De status van het Principes en ontwerpeisen document en het proces beschrijven (in doc en Edustandaard)

- In document verwerkt, nog verwerken op site

Actiepunt #23: TEAMS omgeving en nieuwe structuur

- Afgehandeld

Actiepunt #24: Bespreking HOSA / Edustandaard Toegang

- Gepland

3. Toelichting MORA / Route 21

De vorige keer hebben we de Hoger Onderwijs Sector Architectuur (HOSA) besproken. Deze architectuur heeft het doel betere voorzieningen te realiseren die duidelijk met elkaar samenhangen. We wilde deze keer ook de middelbaar beroepsonderwijs sector architectuur bespreken, maar deze lijkt (nog) niet te bestaan.

Er is wel al een middelbaar beroepsonderwijs referentie architectuur (MORA). De MORA is met name gericht op de interne organisatie. In de MORA is beschreven hoe een mbo-school werkt. Het biedt een gemeenschappelijke structuur en taal om meer samenwerking mogelijk te maken. Het kan gezien worden als een checklist om inzicht te krijgen waar afgeweken wordt van norm. Het biedt basismateriaal voor communicatie naar management voor strategische keuzes en impactanalyses.

De MORA is de opvolger van Triple A en werd voorheen ook wel Route 21 genoemd. De MORA heeft een betere aansluiting op de Hoger Onderwijs Referentie Architectuur (HORA). Het geeft inzicht in welke processen er allemaal lopen en welke informatie er van persoon naar persoon gaan en welke functionaliteiten hiervoor nodig zijn. Het beschrijft niet hoe dit te organiseren.

Er zijn rond de MORA nog wel wat aandachtspunten. Paul licht een aantal aspecten toe.

De MORA geeft het proces weer (bijv. beroepspraktijkvorming), maar niet de criteria die hieraan gesteld (zouden moeten) worden. Welke kaders vanuit een bepaalde wet gelden is vaak niet traceerbaar. Alle processen die door wet afgedwongen worden moeten onderdeel zijn van de MORA.

Er zijn ook aandachtspunten rond semantiek. In het MBO worden andere begrippen gebruikt dan in het HO. Ook tussen onderwijsinstellingen binnen het MBO zijn er soms verschillen. Dit komt soms doordat de gebruikte systemen een bepaald begrip hanteren dat niet (makkelijk) te wijzigen is.

Een ander aandachtspunt betreft de applicatie laag. Het inzicht in wat in welk systeem gebeurt heeft meerwaarde, de praktijk is echter dat systemen zich over het algemeen niet houden aan kaders van een referentiearchitectuur. Leveranciers creëren combinaties van

systemen in hun dienstverlening om vele redenen. Een splitsing of samenvoeging kan soms ook vanuit nieuwe wetgeving ontstaan. Over het algemeen geldt dat dit over de jaren heen een dynamiek kent die niet te mappen is op de applicatielaag van een referentiearchitectuur. De vraag is dus of een applicatielaag in de referentiearchitectuur wenselijk is.

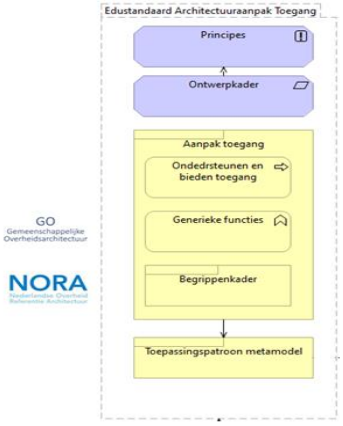
De MORA wordt meer en meer toegepast. Onderwijsinstellingen moeten hier nog wel hun weg in vinden. Er wordt ondersteuning geboden door MBO digitaal

De MORA beschrijft niet het ‘Hoe’, dus ook niet voor toegang. Toch is er ook behoefte aan het ‘Hoe’. Er is hiervoor dan ook een traject gestart als laag boven op de MORA die ook (deels?) het ‘Hoe’ beschrijft.

4. Modellen en deliverables

Deliverables

We hebben reeds een aantal documenten opgesteld. Eerder is gevraagd om deze ook breder te delen (Principes en Ontwerpeisen). Hierbij is wel aangegeven dat deze nog in ontwikkeling zijn. Ook is er overlap in de verschillende documenten. Een deel van ‘Principes en Ontwerpeisen’ is eigenlijk meer een begrippenkader dat wellicht beter bij ‘Architectuuraanpak en concepten’ past. We maken bij het opstellen van de documenten zoveel mogelijk gebruik van bestaand materiaal, zoals NORA en de Gemeenschappelijke Overheidsarchitectuur. Een belangrijk onderdeel zijn de generieke functies die voor de verschillende metamodellen relevant zijn.



ROSA metamodel

We zijn ook in gesprek met het Revisie ROSA project over het ROSA metamodel. Dit heeft ertoe geleid dat we een beter beeld nodig hebben over de verschillende concepten die we de afgelopen tijd al hebben besproken binnen de IAA werkgroep. Om onze gedachten te scherpen hebben we zelf een aantal metamodellen opgesteld op basis van archimate. We onderkennen hierin (voorlopig) het volgende:

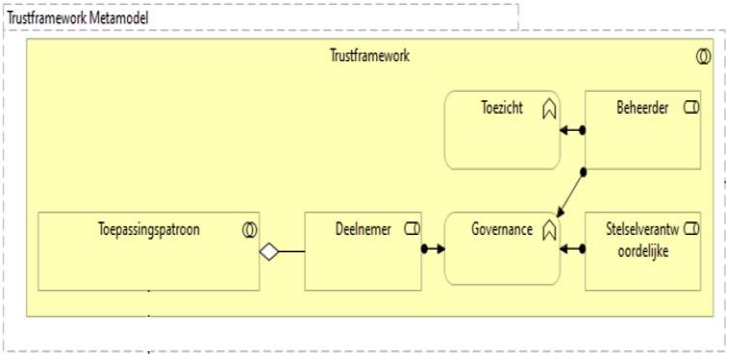
- Trustframework metamodel
- Toepassingspatroon metamodel
- Delen gegevens metamodel
- IBP-metamodel

We hebben hiermee een stap gemaakt om concepten en relaties beter in beeld te krijgen. We kunnen zo ook het gesprek beter aangaan wat in het ROSA metamodel geïntegreerd zou kunnen worden. Het doel van een bepaalde mate van integratie is dat bij de vulling van de ROSA beter gestuurd kan worden op relevante kaders en kunnen we vergelijken op basis van de patronen. We denken vooralsnog met name aan het thema beveiliging (IBP met IAA als een domein hierbinnen) en delen van gegevens (hiermee in de basis kunnen aansluiten op strategische vergezichten als die van de HOSA en huidige inrichtingsvormen zoals federatieve toegang). De uitdaging hierin is om het ROSA metamodel abstract te houden, maar wel een aantal basisconcepten concreet genoeg maken om dit doel te bereiken. De overige metamodellen (toepassingspatroon/trustframework) zijn dan onderdeel van de deliverables van onze Edustandaard werkgroep Architectuuraanpak Toegang.

Trustframework metamodel
We hebben als Edustandaard werkgroep Architectuuraanpak Toegang besloten dat we bestaande en nieuwe afsprakenstelsels en projecten met een nieuwe innovatieve inrichting willen kunnen toetsen in hoeverre deze op elkaar aansluiten. Dit in principe met betrekking tot toegang, maar in bredere zin gaat het om het delen van (persoons)gegevens.

Om deze toets als onderdeel van een ROSA scan te kunnen uitvoeren zijn we aan de slag gegaan met het definiëren van modulaire elementen die zijn samengesteld op basis van patronen. De aanpak is dus een meta-afspraak, vergelijkbaar met bijvoorbeeld MIM (methodiek voor het beschrijven van informatiemodellen) en AMIGO (methodiek om stapsgewijs afspraken te maken voor gegevensuitwisseling).

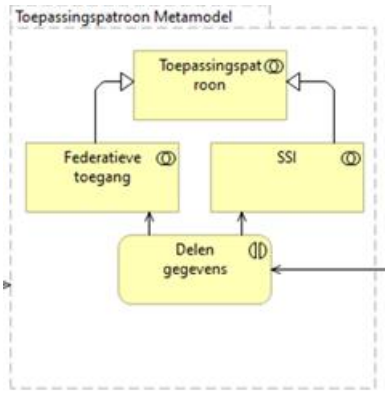
In het trustframework metamodel onderkennen we het gebruik van een bepaald toepassingspatroon voor het delen van gegevens aangevuld met een governancestructuur.



Voorbeelden van trustframeworks binnen het onderwijs zijn bijvoorbeeld SURFconext en Entree Federatie, maar ook OSO[1]. Andere trustframeworks waar we binnen het onderwijs mogelijk gebruik van maken zijn bijvoorbeeld eIDAS en eHerkenning.

Met het definiëren van toepassingspatronen die verschillende trustframeworks gebruiken worden ze vergelijkbaar.

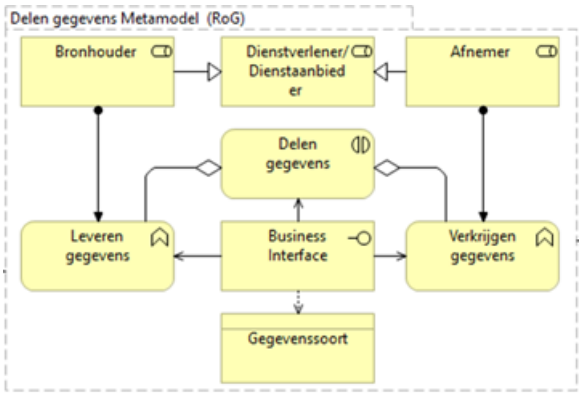
Toepassingspatronen metamodel
Binnen een trustframework worden er afspraken gemaakt over rollen en de interacties hiertussen. Hierbij worden er keuzes gemaakt tussen verschillende toepassingspatronen (inrichtingsvormen). Voor het delen van identiteitsgegevens kan bijvoorbeeld het “federatieve toegang” toepassingspatroon gebruikt worden. Dit toepassingspatroon is bijvoorbeeld gebaseerd op standaarden als SAML of OIDC. Een meer innovatief toepassingspatroon is bijvoorbeeld “Self sovereign identities (SSI)” waarbij de persoon zelf een meer centraal komt te staan. Deze inrichtingsvorm beperkt zich meestal niet tot het delen van identiteitsgegevens.



Doel: De toepassingspatronen bouwen voort op het metamodel delen gegevens. De bronhouder, afnemer, betrokkene en interacties worden meer concreet gedefinieerd. Ze onderscheiden zich o.a. door verschillende aanvullende rollen en (centrale) referentiecomponenten. Over het algemeen maken ze wel gebruik van dezelfde (generieke) functies. Met het definiëren van de generieke functies (GO/NORA) creëren we dus de bouwstenen voor de toepassingspatronen.

[1] Overstapservice Onderwijs (OSO) - Veilig en betrouwbaar leerlinggegevens overdragen (kennisnet.nl)

Delen gegevens metamodel
Zoals eerder aangegeven gaat het bij een toepassingspatroon in de kern om het delen van gegevens, het leveren en het verkrijgen. Het leveren is belegd bij een bronhouder. Dit metamodel vormt de basis voor de verschillende toepassingspatronen. Het metamodel wordt vormgegeven door aspecten uit het document 'Regie op gegevens' en bijvoorbeeld de Data Sharing Coalition.

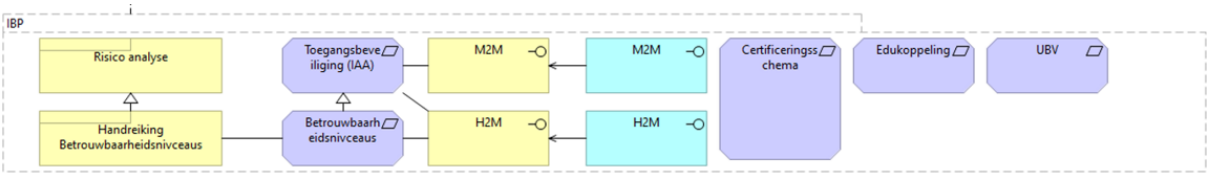


Het document 'Regie op gegevens' beschrijft in principe een trustframework op basis van het SSI-toepassingspatroon. Het gaat er van uit dat de burger steeds meer regie op gegevens gaat voeren. Dit zal in het kader van leven lang leren steeds meer voorkomen en is ook het lange termijn perspectief van de HOSA. Als werkgroep hebben wij onderkend dat dit wenselijk is als de burger in staat is dit te doen, maar dat dit zeker in het PO en VO vaak niet het geval is. Daarom moet ook voorzien is in de situatie dat de burger ontzorgd wordt. Dit is de huidige situatie met federatieve toegang waar de onderwijsinstelling de regie voert. Beide situaties moeten ondersteund kunnen worden, daarom hebben wij onderkend dat er meerdere toepassingspatronen kunnen zijn. Waarbij de infrastructuur die hiervoor nodig is per patroon kan verschillen.

Doel metamodel: In het delen gegevens metamodel willen we de functie van delen expliciet maken en hierbij relevante rollen onderkennen, de bronhouder, afnemer en betrokkene. We willen hiermee onderscheid kunnen maken op werkingsgebied en handelingsbekwaamheid-bevoegdheid van betrokkene. Bijvoorbeeld: Binnen edustandaard is er bijvoorbeeld een OOAPI en Edukoppeling standaard. Wat zijn dit precies, waarom hebben we deze twee standaarden, wat zijn de overeenkomsten en wat verschillen.

IBP
In een eerdere fase hebben het over een aantal zaken gehad die een relatie hebben met informatiebeveiliging en privacy (IBP). We hebben verschillende use cases besproken en een risicoanalyse uitgevoerd op basis van de handreiking betrouwbaarheidsniveaus van Forum standaardisatie. We concludeerde dat een uniform normenkader betrouwbaarheidsniveaus met bijbehorende handreiking voor het onderwijs wenselijk was. Het blijkt echter lastig om hier concreet invulling aan te geven gezien de impact die dit heeft bij onderwijsinstellingen. Een mogelijk alternatief is het gebruik van externe (Nationale) stelsels die een hoger betrouwbaarheidsniveau ondersteunen en waarbij de betreffende doelgroep over het juiste authenticatiemiddel beschikt. We hebben eea rond de risicoanalyse en betrouwbaarheidsniveaus opgenomen in het document 'Architectuuraanpak en concepten'.

De verschillende metamodellen zullen een aantal generieke (M2M en/of H2M) interacties onderkennen waarbij IBP-kaders en maatregelen van toepassing zullen zijn. We willen een aantal zaken die we binnen het onderwijs geregeld hebben (gaan regelen?) expliciet onderkennen in het IBP-metamodel (bijvoorbeeld Certificeringsschema, UBV en Edukopppeling).



5. Rondvraag & afsluiting

Het volgende overleg is op 17 maart 2022 van 15:00 tot 17:00 uur. Op de agenda staan dan de volgende onderwerpen:

- Opening en mededelingen
- Verslag feb 2022 & acties
- Modellen en Regie op Gegevens

6. Actielijst

#	Omschrijving	Status	Einddatum	Actie-houder
5	Voorstel om aanpak uit te breiden met autorisatie rollen en het proxy model	Open		Erwin
8	Kaders voor thema toegang ontwikkelen tbv ROSA scan. We beginnen met principes en we gaan bij voorkeur gebruik maken van bestaande principes voor toegang	Loopt		Bram en Erwin
19	Nadat kaders zijn opgesteld gaan we nog eens door attributentabel, welke tributen zijn wanneer nodig	Open		WG
20	Aan de attributentabel ook de doelen (Audit)Logging en Support toevoegen	Open		Erwin
21	Check eduID op de generieke functies van Principes en ontwerpeisen	Open		Peter
22	De status van het Principes en ontwerpeisen document en het proces beschrijven (in doc en Edustandaard)	Open		Brian/Erwin
24	Bespreking HOSA/ Edustandaard Principes en ontwerpeisen	Gepland		Tom/Menno/Bram/Erwin/…
25	Openbare consultatie NL GOV OpenID Connect profiel en compliance	Open		Peter/SURF

BES = Bureau Edustandaard
Grijs = afgehandeld of vervallen