Projectvoorstel Toekomstbeeld Toegang

Aan	Architectuurraad
Van	Edustandaard Werkgroep IAA
Datum	Mei 2018
Onderwerp	Projectvoorstel Toekomstbeeld Toegang
Status	Concept

Inhoud

1. Inleiding

1.1. Aanleiding en doelstelling

In opdracht van de Standaardisatieraad is er een werkgroep IAA[1] opgericht om te onderzoeken of de toekomstbeelden die op diverse plekken binnen het onderwijsdomein worden ontwikkeld op elkaar aansluiten en in lijn zijn met Rijksbrede ontwikkelingen. Deze werkgroep was breed samengesteld uit diverse onderwijspartijen. Zowel overheid als private partijen waren vertegenwoordigd met een goede inbreng van alle sectoren. De geselecteerde toekomstbeelden zijn redelijk globaal. Daarom zijn van alle sectoren use cases opgesteld om op gedetailleerder niveau de wijze van toegang te kunnen onderzoeken. De werkgroep heeft de toekomstbeelden en use cases met elkaar vergeleken en de overeenkomsten en verschillen geanalyseerd. De analyse heeft voor verschillende aandachtsgebieden een aantal bevindgingen opgeleverd. Voor een aantal bevindingen zijn adviezen geformuleerd, voor overige is nader onderzoek vereist. Deze bevindingen en adviezen zijn gevat in de Notitie Analyse IAA initiatieven[2].

De notitie zal in de Standaardisatieraad van 27 juni 2018 besproken worden. Als opdrachtgever is het aan de Standaardisatieraad om te bepalen hoe met de adviezen en mogelijke vervolgstappen (wie, waar) om te gaan.

In de Architectuurraad van 12 april is besloten dat de Architectuurraad de Standaardisatieraad gaat adviseren over de concrete invulling van de noodzakelijke vervolgstappen. Om te voorkomen dat de opvolging van de adviezen bij verschillende organisaties en ketens tot onwenselijke verschillen gaat leiden vindt de Architectuurraad het wenselijk de onderzoeksvragen voor het hele onderwijsdomein op te pakken. Dat betekent dat op dit vlak ook samenwerking moet ontstaan. De Architectuurraad heeft derhalve besloten een projectvoorstel uit te werken ter agendering bij de volgende Standaardisatieraad. Het voorstel beschrijft hoe je, over alle sectoren heen, de onderzoeksvragen uit de notitie kunt gaan beantwoorden. Dit document bevat het projectvoorstel voor de noodzakelijke vervolgstappen.

1.2. Projectresultaat

Het uiteindelijke projectresultaat is een breed afgestemd Toekomstbeeld Toegang voor het onderwijsdomein. Het beleggen van werkpakketten, waarbij verbinding wordt gezocht met centrale (zoals beheerders routeringsdienst) en decentrale (zoals beheerders authenticatiediensten en dienstaanbieders) rollen, zorgt voor de brede afstemming van het toekomstbeeld. Dit wordt in meer detail beschreven bij de aanpak.

De centrale en decentrale rollen hebben zich in principe gecommitteerd dat relevante kaders meegenomen worden in de roadmap voor de (door)ontwikkeling van hun diensten, maar dit traject vormt geen onderdeel van het project. Bij de projectorganisatie wordt beschreven welke partijen een centrale en/of decentrale rol hebben.

1.3. Afbakening & randvoorwaarden

- De werkpakketten die de werkgroep in dit voorstel heeft opgenomen zijn beperkt tot de onderzoeksvragen zoals die geformuleerd zijn in de Notitie Analyse IAA initiatieven.
- Projectdeelnemers zijn verantwoordelijk voor bepaalde werkpakketten om tot een gezamenlijk Toekomstbeeld Toegang te komen. Het project is niet verantwoordelijk voor de realisatie van dit toekomstbeeld. De projectdeelnemers hebben wel de

[1] https://www.wikixl.nl/wiki/rosa/images/rosa/0/05/Bijlage_7._Voorstel_voor_inventarisatie_en_opstellen_overzicht_IAA.PDF
[2] https://www.wikixl.nl/wiki/rosa/images/rosa/f/f0/Notitie_Analyse_IAA_initiatieven_v0.99.pdf

verantwoordelijkheid om de haalbaarheid van dit toekomstbeeld intern in hun organisatie dan wel achterban te toetsen.

- Het resultaat, een Toekomstbeeld Toegang voor het hele onderwijsdomein, vereist betrokkenheid van alle betrokken partijen binnen alle onderwijssectoren. Zij onderschrijven het Toekomstbeeld of er is inzicht op welke punten dit afwijkt van wat zij wenselijk achten.

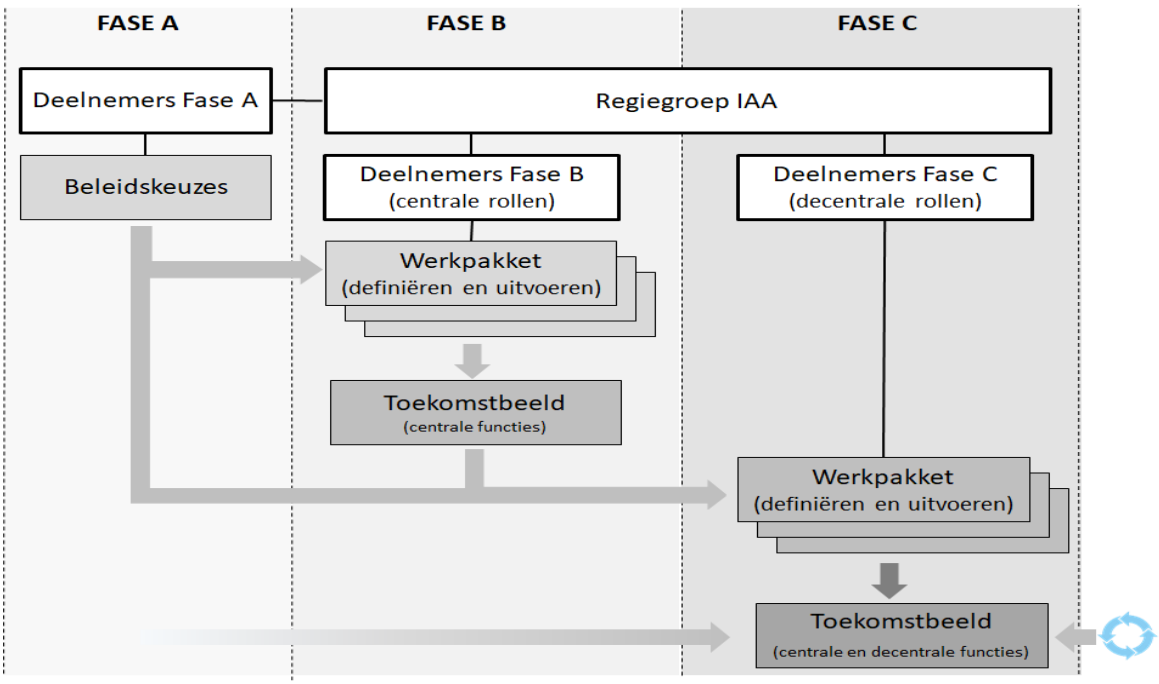
2. Aanpak en resultaten

Het project is gericht op het beleggen van een aantal werkpakketten met als eindresultaat een Toekomstbeeld Toegang voor het hele onderwijsdomein. Er is nu echter geen governance rond toegang ingericht voor het hele onderwijsdomein. De werkpakketten kunnen dus niet integraal bij een bepaald gremium belegd worden. Er wordt daarom met een pragmatisch aanpak gewerkt met het centraal en decentraal beleggen van een aantal werkpakketten. Met deze aanpak wordt het benodigde brede draagvlak gecreëerd doordat de verschillende stakeholders betrokken zijn bij de ontwikkeling ervan. Er wordt wel een centrale regiegroep IAA ingericht die verantwoordelijk is voor het beleggen van de centrale en decentrale werkpakketten bij verschillende gremia en het coördineren van de werkzaamheden en bewaken van de samenhang.

De werkpakketten zijn een vertaling van de onderzoeksvragen van de adviezen uit de notitie. De werkpakketten hebben betrekking op het richten van een IAA stelsel, maar kunnen verschillend van aard en inhoud zijn. Een werkpakket kan bijvoorbeeld het opstellen van een beleidsnotitie zijn die meer achtergrondinformatie geeft om tot een bepaalde keuze te komen. Een ander werkpakket beschrijft meer technisch hoe met het effect van de gekozen multi-middelen strategie in het toekomstbeeld omgegaan kan worden.

In de aanpak wordt er rekening gehouden met het feit dat kaders kunnen wijzigen. Door het toekomstbeeld conform het advies actief onder beheer te houden kan er ook later op basis van nieuwe inzichten bijgestuurd worden. Dit zal wel opnieuw afstemming vereisen met verantwoordelijke en mogelijk wisselende gremia.

Er wordt in drie fasen naar het eindresultaat gewerkt. Dit wordt schematisch weergegeven door Figuur 1.

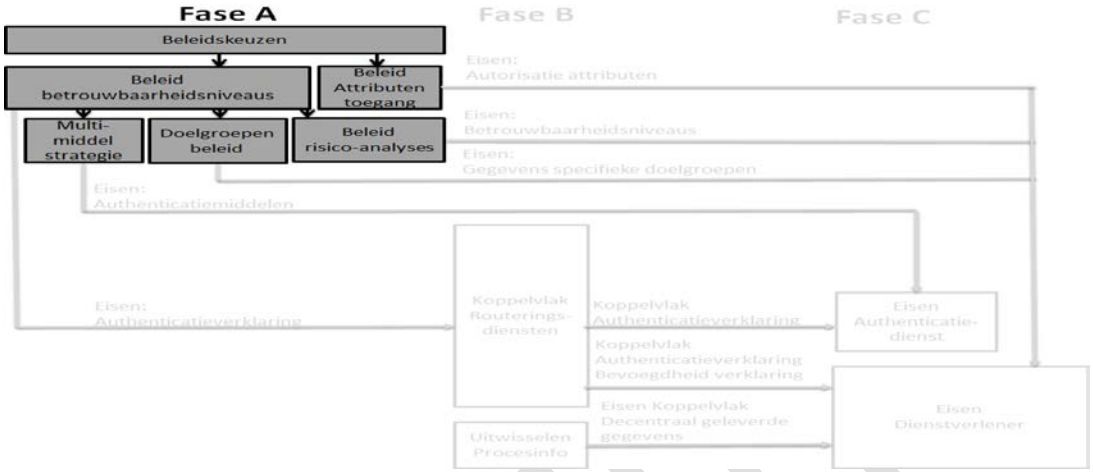


Figuur 1 - Aanpak ontwikkeling toekomstbeeld toegang

2.1. Projectresultaten fase A

De eerste fase heeft betrekking op een aantal beleidskeuzes die in de notitie genoemd worden. Deze vallen niet alle direct onder reikwijdte van de regiegroep. Het proces om tot de betreffende beleidskeuzes te komen die niet onder de reikwijdte van de regiegroep vallen

valt derhalve dan ook niet onder verantwoording van het project. Het gaat hierbij met name om een aantal beleidskeuzes die centraal bij OCW belegd en uitgevoerd worden. De regiegroep is aangehaakt bij deze trajecten om vroegtijdig inzicht te hebben in de uiteindelijke keuzes.



Figuur 2 - Fase A: Beleidskeuzes

De volgende beleidskeuzes zijn onderdeel van fase A:

1. Beleid ten aanzien van betrouwbaarheidsniveaus
2. Beleid ten aanzien van authenticatiemiddelen (multi-middelen strategie)
3. Beleid ten aanzien van doelgroepen
4. Beleid ten aanzien van risicoanalyses
5. Beleid ten aanzien van attributen ten behoeve van toegang

2.1.1. Beleid ten aanzien van betrouwbaarheidsniveaus

Dit beleid vormt een kader voor de multi-middelen strategie en het beleid ten aanzien van doelgroepen. Het is een belangrijk aspect voor het Toekomstbeeld Toegang, de authenticatiemiddelen van dienstafnemers en de risicoanalyses die dienstaanbieders uitvoeren.

- Doel: Zorgt voor een goede aansluiting op Nationale en Europese ontwikkelingen. Het Onderwijsdomein is voorbereid op toenemende regelgeving.
- Resultaat: Notitie met duiding van noodzaak en een voorstel hoe dit beleid te verwezenlijken. Dit werkpakket maakt ook inzichtelijk wat de consequenties zijn, bijvoorbeeld wat dit betekent voor bestaande betrouwbaarheidsniveaus die binnen het onderwijs gebruikt worden.
- Belegd bij Regiegroep IAA

2.1.2. Beleid ten aanzien van authenticatiemiddelen (multi-middelen strategie)

De standaardisatie op eIDAS betrouwbaarheidsniveaus betekent dat vele huidige authenticatiemiddelen binnen het onderwijsdomein als Laag geclassificeerd zullen worden. Er zijn diensten binnen het onderwijs die een hoger betrouwbaarheidsniveau vereisen. Het beleid is gericht op hoe er gebruik kan worden gemaakt van (andere) vereiste authenticatiemiddelen.

Het beleid kan gericht zijn op het toepassen van authenticatiemiddelen zoals geboden door iDIN, Idensys, eHerkenning, een centrale authenticatiedienst voor het onderwijsdomein, of

het toepassen van authenticatiemiddelen van onderwijsinstellingen. Het identificatie- en registratieproces bij onderwijsinstellingen volgt nu niet een procedure conform betrouwbaarheidsniveau substantieel, maar zou hier mogelijk op aangepast kunnen worden. Dit in combinatie met het gebruik van een authenticatiemiddel van betrouwbaarheidsniveau substantieel maakt het mogelijk dat authenticatiediensten van onderwijsinstellingen dit kunnen ondersteunen. Dit kan, in combinatie met een SURFconext en/of Entree Federatie koppeling, als een valide alternatief beschouwd worden.

- Doel: De multi-middelen strategie regelt dat dienstafnemers over authenticatiemidddelen beschikken die het minimale betrouwbaarheidsniveau ondersteunt dat een dienstaanbieder vereist.
- Resultaat: Geen onderdeel van het project. De kaders die uit het beleid volgen moeten wel in de ontwikkeling van het toekomstbeeld meegenomen worden.
- Belegd bij OCW

2.1.3. Beleid ten aanzien van doelgroepen

Er wordt geadviseerd om binnen het onderwijsdomein een gemeenschappelijk beleid voor de belangrijkste doelgroepen op te stellen. De eisen voor toegang kunnen per doelgroep verschillen. Dit speelt sterk bij minderjarige kinderen. Zij kunnen zelf niet om digitale toegang vragen. Hier dient beleidsmatig vastgesteld te worden welke mogelijke randvoorwaarden hiervoor gelden. Dit beleid heeft ook betrekking op onderwijsdeelnemers die niet uit de EU afkomstig zijn.

- Doel: Doelgroepen beschikken over de authenticatiemiddelen en overige gegevens die nodig zijn om toegang tot diensten te verkrijgen.
- Resultaat: Geen onderdeel van het project. De kaders die uit het beleid volgen moeten wel in de ontwikkeling van het toekomstbeeld meegenomen worden.
- Belegd bij OCW

2.1.4. Beleid ten aanzien van risicoanalyses

Er wordt geadviseerd om gemeenschappelijk risico's voor ketens vast te stellen bij risicoanalyses. Een risicoanalyse bepaalt welke maatregelen proportioneel zijn. Bij ketens en verwerking van vergelijkbare gegevens zou de risicoanalyse in dezelfde maatregelen moeten resulteren.

- Doel: De risicoanalyse levert eenduidig te nemen maatregelen op. Diensten en ketens waar dezelfde gegevens verwerkt worden nemen met betrekking tot toegang dezelfde maatregelen.
- Resultaat: Analyse en rapportage hoe dit beleid in te richten. Onderzoeken of de huidige inrichting met het Convenant Digitale Onderwijsmiddelen en Privacy[3] en het Certificeringsschema voldoende is. Worden ketens hierin al onderkend? De maatregelen bij het verlenen van toegang aan externe gebruikers moeten aansluiten op de overige IAA beleidskeuzes, zoals de resulterende eIDAS betrouwbaarheidsniveaus en machtigingen.
- Belegd bij Edustandaard Werkgroep IBP

2.1.5. Beleid ten aanzien van attributen ten behoeve van toegang

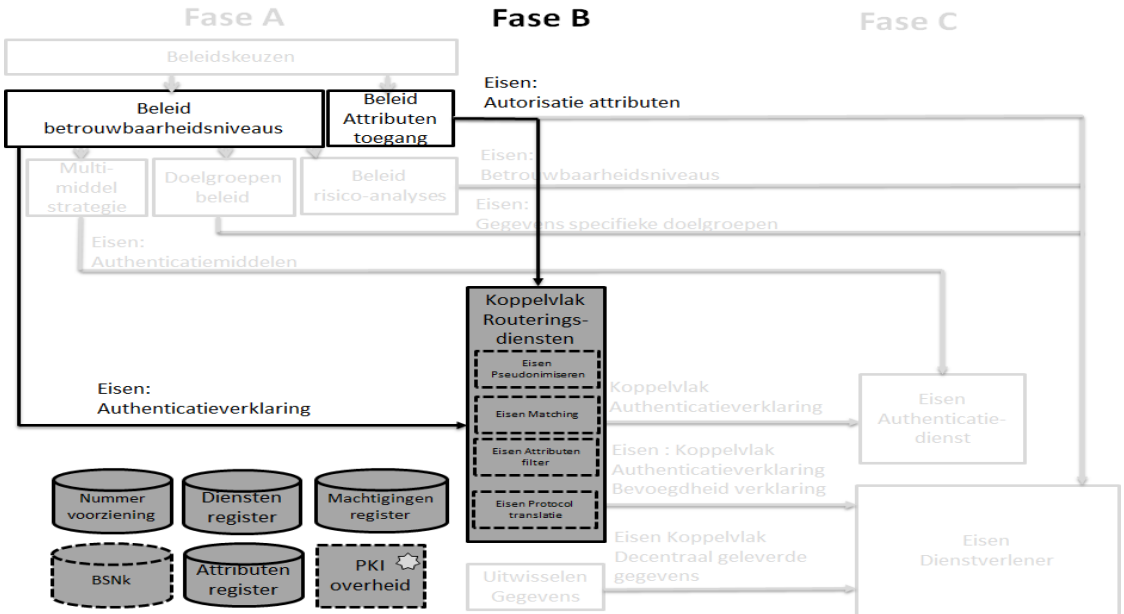
Het is wenselijk om een attributenbeleid ten behoeve van toegang (autorisatie) voor het onderwijsdomein op te stellen. Dit attributenbeleid is richtinggevend voor gegevens die bij toegang worden geleverd via de routeringsvoorziening(en) of via een directe koppeling.

[3] https://www.privacyconvenant.nl/het-convenant/

- Doel: Dataminimalisatie en eenduidigheid rond gegevens die bij toegang t.b.v. de autorisatie geleverd worden.
- Resultaat: Analyse van gegevens die t.b.v. toegang (autorisatie) geleverd worden en hoe dit teruggebracht kan worden tot een minimale set. Het attributenbeleid van Edu-K kan hierbij als basis gebruikt worden. Eventueel wordt ook inzichtelijk gemaakt welke aanvullende gegevens er voor een bepaald proces nodig zijn, maar dit is niet expliciet onderdeel van het werkpakket.
- Belegd bij Regiegroep IAA

2.2. Projectresultaten fase B

In de tweede fase worden werkpakketten uitgevoerd die bij centrale rollen kunnen worden belegd. De uitkomsten van de werkpakketten en de kaderstellende beleidskeuzen uit fase A worden in samenhang vertaald naar een eerste concept Toekomstbeeld Toegang. Het resultaat van deze fase is een concreet beeld rond de centrale rollen, zoals registers en routeringsdiensten en hun koppelvlakken.



Figuur 3 -Fase B: Werkpakketten centrale rollen

De volgende werkpakketten zijn onderdeel van fase B:

1. Eisen vanuit beleid betrouwbaarheidsniveaus
2. Eisen attributenbeleid ten behoeve van toegang
3. Visie op pseudonimiseren
4. Visie op machtigen

2.2.1. Eisen vanuit beleid betrouwbaarheidsniveaus op authenticatieverklaring

Het betrouwbaarheidsniveau van de authenticatieverklaring van routeringsdiensten onderkennen nu geen of een ander betrouwbaarheidsniveau dan die eIDAS hanteert. Dienstaanbieders kunnen op basis van de bij de risicoanalyse vastgestelde minimale betrouwbaarheidsniveau dit niet als eis aan routeringsdienst doorgeven.

- Doel: Routeringsdiensten kunnen conform het beleid rond betrouwbaarheidsniveaus authenticatieverklaringen leveren.

- Resultaat: Kaders voor de routeringsdienst en de te leveren authenticatieverklaring zijn inzichtelijk gemaakt. Deze kaders zijn onderdeel van het Toekomstbeeld Toegang.

2.2.2. Eisen attributenbeleid ten behoeve van toegang

Het is wenselijk om een attributenbeleid ten behoeve van toegang (autorisatie) op te stellen dat bruikbaar is voor alle digitale diensten binnen het onderwijs. Dit attributenbeleid is dan richtinggevend voor gegevens die bij toegang geleverd moeten kunnen worden. De keuze hierin hebben consequenties voor de filterfunctie van de centrale rollen.

De centrale rollen leveren bij toegang een generieke set gegevens aan een bepaalde dienstaanbieder zonder dat hier per dienst/proces in gevarieerd kan worden. Overige gegevens worden niet (noodzakelijk) via de centrale rol geleverd. Voor een specifieke dienst/proces kunnen aanvullende gegevens op basis van doelbinding geleverd worden. Een centraal attributenregister maakt inzichtelijk welke gegevens er uitgewisseld kunnen worden.

- Doel: Dataminimalisatie en eenduidigheid rond attributen voor toegang.
- Resultaat: Het toekomstbeeld beschrijft de attributen die bij toegang via centrale rollen geleverd moeten kunnen worden. Voor de Edu-K keten is dit al gerealiseerd. Het Toekomstbeeld Toegang heeft echter een bredere scope en vraagt bredere afstemming.

2.2.3. Visie op pseudonimiseren

De multi-middelen strategie geeft inzicht in gebruikte authenticatiemiddelen. In huidige situatie worden verschillende authenticatiemiddelen gebruikt en is de vorm van pseudonimisering hier vaak aan gekoppeld. Die vorm wordt mogelijk door de routeringsdienst bepaald. Voor een bepaald pseudoniem is het (gewenste) werkgingsgebied niet vastgesteld. Dit leidt tot problemen, bijvoorbeeld bij studenten- en medewerker mobiliteit.

Binnen het onderwijs worden er ketenpseudoniemen gebruikt en bij de digitale overheid zet men in op zogenaamde polymorfe pseudoniemen. De routeringsdiensten SURFconext en Entree Federatie gebruiken verschillende vormen om een overgangen te ondersteunen van het ene (IdP) naar het andere domein (SP) en leveren soms verschillende identifiers in dezelfde sessie.

Op welke aspecten de routeringsdienst de dienstaanbieders ontzorgt is een beleidskeuze. Hieronder vallen bijvoorbeeld de overgangstermijnen om van oude naar nieuwe koppelvlakken over te gaan.

Verschillende vormen van pseudoniemen hebben verschillende karakteristieken en hiermee verschillende voor- en nadelen. Wanneer wordt bij voorkeur een bepaalde vorm toegepast? Wat is het gewenste bereik van een bepaalde vorm en moeten er in bepaalde gevallen overgangen worden ondersteund? Willen we een routeringsdienst zo inrichten dat deze altijd een door dienstaanbieder aangegeven vorm kan leveren? Wat zijn de consequenties van deze keuzes op de routeringsdienst?

- Doel: Het voorkomen van problemen rond o.a studenten- en medewerker mobiliteit.
- Resultaat: Analyse van gebruikte authenticatiemiddelen door verschillende gebruikersgroepen en de pseudoniemen die de dienstaanbieder geleverd krijgt. Inzicht in de rol van de routeringsdienst hierbij en de kaders die hieraan gesteld worden. Op basis hiervan wordt er een beeld geschetst van de werkingsgebieden

van pseudoniemen en mogelijke overgangen. Het resultaat vormt een onderdeel van het Toekomstbeeld Toegang.

2.2.4. Visie op machtigen

Er zijn situaties waarbij een bepaalde partij zijn bevoegdheden bij een bepaalde dienst wil kunnen overdragen aan een andere partij (persoon, organisatie, applicatie). De dienstaanbieder wil bij toegang kunnen vaststellen of sprake is van overdracht van bevoegdheden en wil deze kunnen verifiëren. Een voorbeeld hiervan is een dienstafnemer die namens een bepaalde organisatie de dienst afneemt. Ook binnen het onderwijsdomein komt dit scenario voor. Het gaat hierbij in principe om het (tijdelijk) overdragen van bevoegdheden en deze bevoegdheden moeten bij toegang gevalideerd kunnen worden.

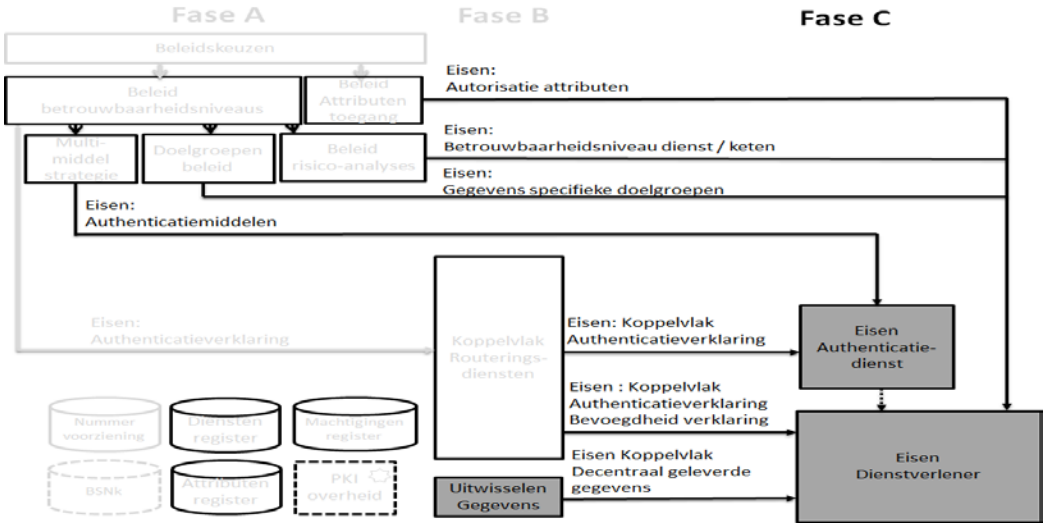
Een centraal (gefedereerd) register voor de registratie van machtigingen lijkt wenselijk. Hoe worden deze geleverd (via routeringsdienst of direct) en dienen deze bij een register geverifieerd te worden of worden deze in een digitale ondertekende verklaring geleverd? Komt er een centraal dienstenregister dat inzichtelijk maakt welke diensten (portalen) er zijn en kunnen de identiteiten die hierin geregistreerd staan mogelijk een rol spelen binnen het machtigingen register?

Het is wenselijk om aan te sluiten bij Rijksbrede ontwikkelingen rond machtigen, maar daar wordt nog gewerkt aan een toekomstbeeld. En de eisen die gesteld worden aan machtigen kunnen per domein sterk verschillen.

- Doel: Eenduidigheid welke vormen van machtigen binnen het onderwijs nodig zijn en duidelijkheid wat de rol van een routeringsdienst hierbij is.
- Resultaat: Generiek model van machtigingsvormen voor gebruikersgroepen. De resulterende architectuurkaders zijn onderdeel van het toekomstbeeld toegang. Hierin wordt duidelijk aangegeven hoe machtigingen geleverd en gevalideerd worden en de rol van de routeringsdienst hierbij.

2.3. Projectresultaten fase C

In de derde fase worden werkpakketten uitgevoerd die bij partijen kunnen worden belegd die decentrale rollen vervullen in het stelsel. De uitkomsten van fase B geven in concept weer wat centraal geregeld wordt. In fase C wordt de impact hiervan met die partijen afgestemd en vastgelegd in het Toekomstbeeld Toegang. Het resultaat van deze fase zijn kaders voor de decentrale rollen zoals authenticatiediensten en dienstaanbieders.



Figuur 4 – Fase C: Werkpakketten decentrale rollen

De volgende werkpakketten zijn onderdeel van fase C:

1. Eisen autorisatie-attributen
2. Eisen betrouwbaarheidsniveau dienst en keten
3. Eisen gegevens specifieke doelgroepen
4. Eisen authenticatiemiddelen
5. Eisen koppelvlak(ken) authenticatieverklaring
6. Eisen bevoegdheid verklaring
7. Eisen koppelvlak decentraal geleverde gegevens

2.3.1. Eisen autorisatie-attributen

Het beleid ten aanzien van attributen voor autorisatie heeft in fase 2 inzichtelijk gemaakt welke attributen er centraal ontsloten moeten kunnen worden. In deze fase wordt dit met beheerders van authenticatiediensten en dienstaanbieders afgestemd. Een authenticatiedienst moet deze kunnen leveren en de dienstaanbieder krijgt deze direct of via de centrale routeringsdienst geleverd.

Dit heeft tevens een relatie met het koppelvlak decentraal geleverde gegevens. Binnen dat werkpakket wordt met dienstaanbieders besproken of en hoe andere gegevens via decentrale koppelvlakken geleverd kunnen worden.

- Doel: Consolideren van de resultaten uit de vorige fase en een bredere afstemming.
- Resultaat: De bij fase 1 en 2 in het toekomstbeeld toegang opgenomen attributen voor toegang zijn breder afgestemd.

2.3.2. Eisen betrouwbaarheidsniveau dienst en keten

Het beleid ten aanzien van de risicoanalyses zorgt voor een gemeenschappelijke kijk op risico's en te nemen maatregelen. De resultaten van fase 2 zijn belegd bij de IBP werkgroep en hierbinnen vindt al afstemming plaats met decentrale partijen zoals dienstaanbieders.

- Doel: Consolideren van de resultaten uit de vorige fase en een bredere afstemming.
- Resultaat: Waar relevant sluiten de maatregelen uit het certificeringsschema aan op IAA aspecten, zoals vereiste betrouwbaarheidsniveau externe dienstafnemers.

2.3.3. Eisen gegevens specifieke doelgroepen

Het beleid rond specifieke doelgroepen bepaald welke verklaringen/gegevens voor een bepaalde doelgroep geleverd moeten kunnen worden.

- Doel: Zorgen dat de vereiste gegevens en verklaringen voor doelgroepen ondersteund worden.
- Resultaat: Het Toekomstbeeld beschrijft de verschillende doelgroepen en de eisen die hieruit volgen.

2.3.4. Eisen authenticatiemiddelen

De multi-middelen strategie bepaald welke authenticatiemiddelen door de authenticatiediensten ondersteund moeten kunnen worden. Hier wordt tevens gekeken welke mate van standaardisatie mogelijk is, bijvoorbeeld door het toepassen van FIDO[4].

- Doel: Zorgen dat de te gebruiken authenticatiemiddelen door authenticatiediensten ondersteund worden.
- Resultaat: Het Toekomstbeeld geeft inzicht in de eisen die aan de authenticatiedienst gesteld worden ten aanzien van de te gebruiken authenticatiemiddelen.

2.3.5. Eisen koppelvlak(ken) authenticatieverklaring

In fase 2 zijn de eisen rond de authenticatieverklaring vastgesteld en deze hebben met name betrekking op het betrouwbaarheidsniveau, het type pseudoniem en de attributen die ten behoeve van toegang hierin meegeleverd moeten kunnen worden. In deze fase wordt met de authenticatiediensten en dienstaanbieders het koppelvlak bepaald waarmee deze verklaring geleverd wordt.

Voor vele IAA koppelvlakken wordt nu het SAML protocol gebruikt. In de notitie wordt geadviseerd om daarnaast bij de routeringsdiensten OpenID Connect (OIDC[5]) te ondersteunen. De authenticatiediensten kunnen mogelijk de authenticatieverklaring op basis van het SAML protocol leveren en hiermee wordt de noodzaak voor een protocoltranslatiefunctie bij de routeringsdienst relevant.

In deze fase willen we bereiken dat er duidelijkheid komt rond de te ondersteunen protocollen. Daarnaast willen we binnen deze protocollen verder standaardiseren rond de toe te passen pseudoniemen, betrouwbaarheidsniveaus en attributen voor toegang.

De SAML en OIDC protocollen zijn niet volledig gespecificeerd en er zijn specifieke onderwijs gerelateerde gegevens nodig. Binnen dit werkpakket wordt duidelijk wat authenticatiediensten moeten ondersteunen.

- Doel: Eenduidig beeld hoe de authenticatieverklaring geleverd wordt
- Resultaat: In het toekomstbeeld is opgenomen welke koppelvlakken de authenticatiediensten, routeringsdiensten en dienstaanbieders moeten kunnen ondersteunen.

2.3.6. Eisen bevoegdheid verklaring

Bij bepaalde scenario's is het van belang dat bij toegang ook betrouwbaar kan worden vastgesteld namens welke partij een dienst afgenomen wordt. Er kan onderscheid gemaakt worden tussen horizontale machtigingen en verticale machtigingen. Horizontale machtigingen zijn machtigingen tussen privé personen en rechtspersonen en tussen rechtspersonen onderling. Verticale machtigingen betreffen de machtigingsstructuur binnen een organisatie. Het gaat hierbij in principe om het (tijdelijk) overdragen van bevoegdheden van de ene partij naar een andere. Deze bevoegdheden moeten bij toegang gevalideerd kunnen worden.

Het is wenselijk om aan te sluiten bij Rijksbrede ontwikkelingen, maar daar wordt nog gewerkt aan een toekomstbeeld. We gaan er wel vanuit dat de eisen per domein sterk verschillend zullen zijn, de kaders die vanuit het onderwijs worden gesteld moeten duidelijk worden.

[4] https://fidoalliance.org/
[5] http://openid.net/connect/

- Doel: Inzichtelijk maken welke vormen van machtigingen binnen het onderwijs noodzakelijk zijn en hoe de ondersteuning hiervan gerealiseerd kan worden.
- Resultaat: Het toekomstbeeld bevat kaders om de gewenste vormen van machtigen te ondersteunen.

2.3.7. Eisen koppelvlak decentraal geleverde gegevens

Er zijn verschillende standaarden rond toegang (leveren identiteitsinformatie) en ter ondersteuning van het proces (alle overige gegevens) beschikbaar en sommige hebben hetzelfde werkings- en toepassingsgebied. Soms is flexibiliteit gewenst en is het wenselijk om dezelfde gegevens via meerdere standaarden, bijvoorbeeld via centrale routeringsdienst, te ontsluiten. In andere gevallen ligt de voorkeur bij een directe koppeling omdat de gegevens sterk variëren.

- Doel: Eenduidige beeld van standaarden en het werkings- en toepassingsgebied.
- Resultaat: Het toekomstbeeld bevat een aantal criteria welke bepalen welke standaard(en) er in een bepaalde context toegepast kan/moet worden.

2.4. Projectorganisatie

De projectorganisatie wordt gevormd door verschillende partijen binnen het onderwijsdomein. Afhankelijk van de fase en sectoren worden de werkpakketten bij verschillende gremia belegd. Een overzicht van de deelnemers wordt weergegeven in de onderstaande tabel.

Fase	Deelnemers	Sectoren	Verantwoordelijkheden
A	OCW, Edustandaard Werkgroep IBP, Regiegroep IAA	PO, VO, MBO, HO	Beleidskeuzen IAA
B en C	Regiegroep IAA	PO, VO, MBO, HO	Rapporteert inhoudelijk aan Architectuurraad en op hoofdlijnen aan de Standaardisatieraad. Coördinatie werkpakketten en deze beleggen bij verschillende gremia. Bewaken van afhankelijkheden en kritieke paden bij centrale en decentrale onderzoeksvragen.
B	Kennisnet, SURF, Raden (?), DUO, Basispoort (?)	PO, VO, MBO	Uitvoeren centrale werkpakketten PO, VO, MBO
B	SURF, Studielink, DUO	HO	Uitvoeren centrale werkpakketten HO
C	VDOD, GEU	PO, VO, MBO, HO	Uitvoeren decentrale werkpakketten PO, VO, MBO, HO

3. Planning