# Projectvoorstel Toekomstbeeld Toegang

| | |
|---|---|
| Aan | Edustandaard Standaardisatieraad |
| Van | Edustandaard Architectuurraad |
| Datum | Juli 2018 |
| Onderwerp | Projectvoorstel  Toekomstbeeld Toegang |
| Status | Concept |

## Inhoud

# 1. Inleiding

## 1.1. Aanleiding en doelstelling

De digitalisering neemt toe en als gevolg hiervan zien we ook een toename in regelgeving. Er worden steeds hogere eisen gesteld aan het borgen van privacy. Voorbeelden hiervan zijn de Algemene Verordening Gegevensbescherming[1], de Wet Digitale Overheid[2] (DO, voorheen GDI) en eIDAS[3] (Electronic Identities And Trust Services). In opdracht van de Standaardisatieraad is er een werkgroep IAA[4] opgericht om te onderzoeken of de verschillende toekomstbeelden rond Identificatie, Authenticatie en Autorisatie (IAA) 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 bevindingen opgeleverd. Voor een aantal bevindingen zijn adviezen geformuleerd, voor de overige is nader onderzoek vereist. Deze bevindingen en adviezen zijn gevat in de Notitie Analyse IAA initiatieven[5].

De notitie is goedgekeurd binnen de Architectuurraad van 21 juni en de Standaardisatieraad van 27 juni. De Architectuurraad heeft de Standaardisatieraad geadviseerd om een projectplan op te stellen om gezamenlijk invulling te geven aan de adviezen en onderzoeksvragen. Hiervoor is een projectvoorstel gemaakt dat op 27 juni is besproken in de Standaardisatieraad. De Standaardisatieraad heeft gevraagd om het projectvoorstel op een aantal punten aan te scherpen. De werkgroep IAA krijgt de opdracht conform dit aangescherpte projectvoorstel een projectplan op hoofdlijnen op te stellen dat besproken zal worden in de Standaardisatieraad van november.

Omdat nu voorzien is dat onderwijsinstellingen niet direct als deelnemer betrokken zijn, wordt geadviseerd om dit projectvoorstel ook af te stemmen met de bestuurlijke overlegorganen van de verschillende sectoren (PO-raad, VO-raad, MBO-raad, VH en VSNU).

## 1.2. Projectresultaat

Het uiteindelijke projectresultaat is een breed gedragen plan om te komen tot een samenhangend Toekomstbeeld Toegang voor het onderwijsdomein. Het beleggen van werkpakketten zorgt voor dat de toekomstbeelden die binnen het onderwijsdomein gebruikt worden op elkaar gaan aansluiten. Daarbij wordt de verbinding gezocht met centrale (zoals beheerders routeringsdienst) en decentrale (zoals beheerders authenticatiediensten en dienstaanbieders) rollen. Dit wordt in meer detail beschreven bij de aanpak.

## 1.3. Afbakening & randvoorwaarden

- De werkpakketten geven aan waar de onderzoeksvragen uit de Notitie Analyse IAA initiatieven belegd worden.
- De adviezen uit de Notitie Analyse IAA initiatieven vormen kaders voor deze werkpakketten.

[1] http://europa.eu/rapid/press-release_IP-18-386_en.htm en https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving
[2] https://www.digitaleoverheid.nl/voorzieningen/identificatie-en-authenticatie/eid/wet-gdi/
[3] https://www.digitaleoverheid.nl/dossiers/eidas/
[4] https://www.wikixl.nl/wiki/rosa/images/rosa/0/05/Bijlage_7._Voorstel_voor_inventarisatie_en_opstellen_overzicht_IAA.PDF
[5] https://www.wikixl.nl/wiki/rosa/images/rosa/f/f0/Notitie_Analyse_IAA_initiatieven_v0.99.pdf

- De regiegroep is verantwoordelijk voor het sturen op samenhang tussen de verschillende toekomstbeelden. De regiegroep is niet verantwoordelijk voor de realisatie van de toekomstbeelden.
- De projectdeelnemers worden door Standaardisatieraad bepaald (deelnemers fase B en C).
- De projectdeelnemers hebben de verantwoordelijkheid om de haalbaarheid van dit toekomstbeeld (of relevante aspecten hiervan) 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.

### 1.4. Governance

Bij de inventarisatie is gebleken dat er binnen het onderwijsdomein verschillende toekomstbeelden worden ontwikkeld die niet op elkaar aansluiten. Er is behoefte aan een gemeenschappelijk Toekomstbeeld. De inventarisatie heeft ook uitgewezen welke vragen beantwoord moeten worden om te komen tot een gemeenschappelijk Toekomstbeeld. Hiervoor moet een plan worden opgesteld. Op basis van dit plan moet een Toekomstbeeld worden ontwikkeld en dit Toekomstbeeld moet gerealiseerd worden. Dit brengt de vraag van het eigenaarschap naar voren. Een Toekomstbeeld heeft alleen waarde als het wordt gerealiseerd. Er is echter niet één bepaalde partij die eigenaar is van het Toekomstbeeld Toegang. Edustandaard is de enige plaats waar iedereen aan tafel zit en waar gestuurd kan worden op samenhang.

Binnen Edustandaard is besloten om de werkgroep Toegang een projectvoorstel op hoofdlijnen op te laten stellen dat aangeeft op welke wijze keuzes gemaakt kunnen worden die er voor zorgen dat de verschillende toekomstbeelden op elkaar gaan aansluiten. Er zijn dus meerdere toekomstbeelden, elk met een eigenaar. De eigenaar kan het bestuur van een organisatie zijn. Bij organisaties als Kennisnet en SURF wordt het bestuurd gevormd door meerdere organisaties die gezamenlijk het bestuur uitmaken. Tevens werken organisaties samen binnen een sector of keten. De “eigenaar” van een toekomstbeeld zal vaak een gremium zijn waarin meerdere organisaties vertegenwoordigd zijn, bijvoorbeeld ketenregie overleggen binnen een sector of een samenwerkingsverband als EDU-K. De organisaties die deel uitmaken van Edustandaard zijn ook vertegenwoordigd binnen de gremia waarin besluiten kunnen worden genomen over de toekomstbeelden. Maar vaak gaat het om andere mensen. Over het algemeen zal een lid van de Standaardisatieraad niet het mandaat hebben om besluiten te nemen over een toekomstbeeld. Daarom heeft de Standaardisatieraad gevraagd om in het projectplan aandacht te besteden aan de governance, mede om de eigenaar te betrekken.

Bij het projectvoorstel worden 3 rollen onderscheiden:

- Regieteam
  Het regieteam is verantwoordelijk voor het sturen op samenhang. De verantwoordelijkheid van het regieteam is om het proces te bewaken waarbij werkpakketten worden belegd bij uitvoerders van werkpakketten en afspraken worden gemaakt over het betrekken van de eigenaren. Daarnaast zorgt het regieteam voor inhoudelijke samenhang. Hierbij wordt bewaakt dat de resultaten van de werkpakketten op elkaar aansluiten. De leden van het regieteam zijn aangewezen door hun vertegenwoordiger in de Standaardisatieraad. De leden van het regieteam moeten beschikken over inhoudelijke expertise en het mandaat hebben binnen hun eigen organisatie mensen te betrekken die nodig zijn voor het opstellen van het projectplan;

- Uitvoerders van werkpakketten
  In het projectplan worden werkpakketten benoemd die belegd worden bij uitvoerders. De uitvoerder kan een organisatie zijn of een samenwerkingsverband waar meerdere organisaties betrokken zijn. De werkpakketten leiden tot gezamenlijke keuzes. Deze gemeenschappelijke keuzes moeten leiden tot aanpassing van toekomstbeelden en het opstellen van een roadmap om van de eigen naar de gewenste situatie te komen. Bij de uitwerking van het projectplan zal de uitvoerders gevraagd worden voor welk toekomstbeeld de aanpassing consequenties heeft, wie hiervan de eigenaar is en welk proces gevolgd moet worden om het commitment van de eigenaar te krijgen voor de beoogde wijzigingen.

- Eigenaars van toekomstbeelden
  Op basis van de input van de uitvoerders wordt inzichtelijk welke eigenaars moeten instemmen met het projectplan en welk proces hiervoor gevolgd moet worden. Deze input gebruikt de regiegroep om te zorgen dat de mening van de betrokken eigenaars wordt meegenomen bij het opstellen van het projectplan. Dit heeft consequenties voor de scope.

### 1.5. Projectorganisatie

De projectorganisatie wordt gevormd door verschillende partijen binnen het onderwijsdomein die bij één of meer fase betrokken zijn. De werkpakketten kunnen niet integraal bij één bepaald gremium belegd worden en er wordt daarom met een gefaseerde aanpak gewerkt (zie aanpak).

In dit voorstel zijn al een aantal deelnemers opgenomen, maar de formele vaststelling van deelnemers wordt door de Standaardisatieraad bepaald. Er wordt geadviseerd om middels vertegenwoordiging tevens de onderwijsinstellingen bij dit project te betrekken. Afhankelijk van de fase en sectoren worden de werkpakketten bij verschillende gremia belegd. Een overzicht van de beoogde deelnemende organisaties en gremia wordt weergegeven in de onderstaande tabel.

| Fase | Deelnemers | Sectoren | Verantwoordelijkheden |
|---|---|---|---|
| A, B en C | OCW<br>PO-Raad<br>VO-raad<br>MBO Raad<br>SURF<br>VSNU<br>VH<br>Kennisnet<br>Werkgroep IBP | 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. Wordt ingevuld door de huidige Edustandaard IAA werkgroep met aanvullingen |
| B | Kennisnet, SURF, DUO, Basispoort | PO, VO, MBO | Uitvoeren centrale werkpakketten PO, VO, MBO |
| B | SURF, Studielink, DUO | HO | Uitvoeren centrale werkpakketten HO |

| | | | |
|---|---|---|---|
| C | VDOD, GEU, CvTE | PO, VO, MBO, HO | Uitvoeren decentrale werkpakketten PO, VO, MBO, HO |

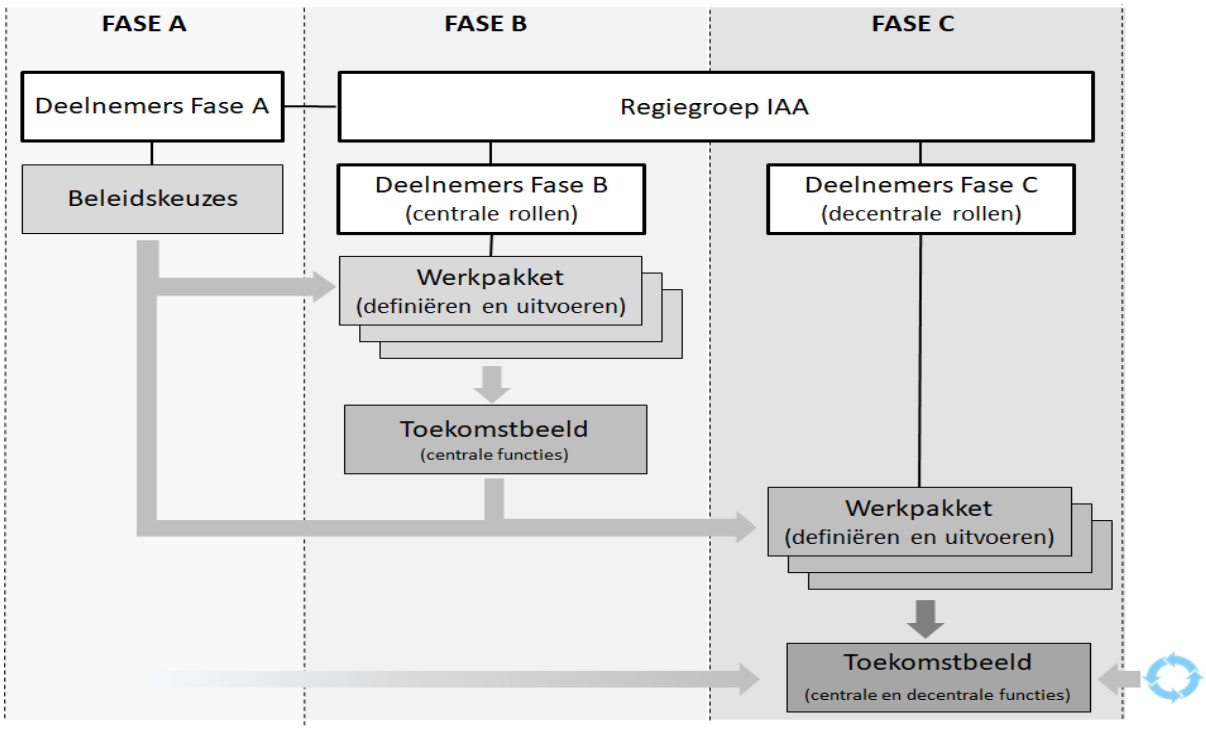
## 2. Aanpak en resultaten

Het project is gericht op het beleggen van een aantal werkpakketten met als eindresultaat een Toekomstbeeld Toegang voor het hele onderwijsdomein. In hoofdstuk governance staat beschreven op welke wijze de governance in het projectplan wordt uitgewerkt en wordt tevens ingegaan op de rolverdeling bij de uitwerking van het projectplan tussen regiegroep, werkgroepen en eigenaren. De regiegroep is tevens verantwoordelijk voor rapporteren van de tussenresultaten aan de Architectuurraad. De Architectuurraad bepaalt de agendering in de Standaardisatieraad, de Standaardisatieraad bekrachtigd.

De onderzoeksvragen uit de notitie zijn gevat binnen de verschillende werkpakketten. De adviezen uit de notitie vormen de initiële kaders. De werkpakketten in de verschillende fases hebben afhankelijkheden naar elkaar. De werkpakketten in fase B en C zijn deels afhankelijk van de beleidskeuzes. Gezien de pragmatische aanpak wordt er voorgesteld om fase A en B gelijktijdig te starten. De adviezen uit de notitie gelden zodoende als initieel kader voor fase B totdat de daadwerkelijke beleidskeuze is gemaakt. Afwijkingen hierop vormen dus een risico, maar het vroegtijdig kunnen starten met fase B weegt zwaarder.

Verder wordt in de aanpak er rekening mee gehouden dat kaders kunnen wijzigen. In de notitie wordt ook aangegeven dat ontwikkelingen elkaar steeds sneller opvolgen. Het Toekomstbeeld Toegang moet dan ook conform het advies actief onder beheer blijven. Het abstractieniveau hiervan biedt verder de benodigde mate van flexibiliteit. Bij de stap naar realisatie is het wel van belang dat de kaders van Toekomstbeeld Toegang worden gevormd door beleidskeuzes en niet adviezen.

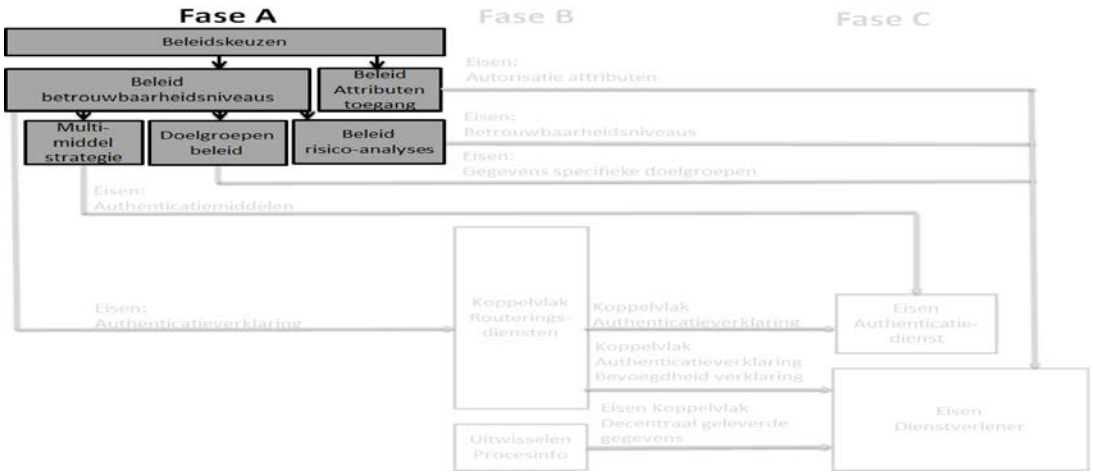
Er wordt in drie fasen naar het eindresultaat gewerkt. Dit wordt schematisch weergegeven door Figuur 1.




Figuur 1 - Aanpak ontwikkeling toekomstbeeld toegang

## 2.1. Projectresultaten fase A

De werkpakketten van fase A zijn bedoeld om een aantal adviezen uit de notitie te borgen binnen het beleid. Het gaat hierbij bijvoorbeeld om werkpakketten rond authenticatiemiddelen en doelgroepen die bij OCW belegd zijn. Het streven is om voor alle sectoren dezelfde beleidskeuzes te maken. Binnen deze fase is dan ook vertegenwoordiging vanuit alle sectoren van belang. De beleidskeuzes vormen de kaders voor fase B. Mocht in fase A er per sector toch verschillende beleidskeuzes zijn gemaakt, dan zal in fase B de impact hiervan bepaald moeten worden.




Figuur 2 - Fase A: Beleidskeuzes

De volgende beleidskeuzes zijn onderdeel van fase A:

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

### 2.1.1. Beleid ten aanzien van betrouwbaarheidsniveaus

Een beleid ten aanzien van betrouwbaarheidsniveaus is wenselijk in verband met Wet Digitale Overheid (voorheen GDI). Op grond van het wetsvoorstel wordt er bij OCW een aansluitschema voor het Onderwijsdomein gemaakt. Hiermee wordt inzicht verstrekt in welke organisaties binnen het onderwijsdomein welke digitale authenticatieprocessen hebben, met welke betrouwbaarheidsniveaus. Het aansluitschema is een vervolg van de GDI analyse die de onderwijssector eerder heeft uitgevoerd. Het maakt duidelijk voor welke diensten toegang via het eID stelsel zal moeten verlopen en waar in het onderwijsdomein precies het betrouwbaarheidsniveau substantieel aan de orde is. Conform het advies uit de notitie wordt hierbij de eIDAS indeling voor betrouwbaarheidsniveaus gehanteerd. Het Onderwijsdomein is hiermee in de basis voorbereid op toenemende regelgeving.

Een ander aspect van dit werkpakket is het vaststellen wat voor consequenties dit heeft voor de huidige betrouwbaarheidsniveaus. Het werkpakket rond de risicoanalyse levert de middelen op om vast te kunnen stellen welk betrouwbaarheidsniveau voor een bepaalde dienst gehanteerd zou moeten worden.

Dit beleid vormt een kader voor de multi-middelen strategie, het beleid ten aanzien van doelgroepen en beleid ten aanzien van risicoanalyses. 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.
- **Advies notitie:** Volg eIDAS indeling voor betrouwbaarheidsniveaus: laag, substantieel en hoog.
- **Resultaat:** Aanduiding waar in het onderwijsdomein de betrouwbaarheidsniveaus substantieel en hoog aan de orde zijn. Een invoeringsstrategie maakt de consequenties inzichtelijk. Dit geeft ook de andere trajecten, zoals beleid ten aanzien van risicoanalyses meer achtergrondinformatie. Ook moet duidelijk worden wat dit betekent voor bestaande betrouwbaarheidsniveaus die nu binnen het onderwijs gebruikt worden.
- **Belegd bij:** OCW, regiegroep IAA en Edustandaard Werkgroep IBP. Door beleggen van werkpakket bij de EdustandaardIBP werkgroep is indirect aanhaking van leveranciers geborgd.

### 2.1.2. 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. Er wordt aangegeven in hoeverre en waar een risico-nemende strategie kan worden gehanteerd en waar een risico-vermijdende strategie past. Bij ketens en verwerking van vergelijkbare gegevens zou de risicoanalyse in dezelfde maatregelen rond toegang moeten resulteren. We streven naar het creëren van een overzicht met alle ketens. En per keten moet op basis van een risico-analyse worden bepaald welk beveiligingsniveau nodig is.

- **Doel:** De risicoanalyse levert eenduidig te nemen maatregelen op voor welke te verwachten schade (kans x impact). Diensten en ketens waar dezelfde gegevens verwerkt worden nemen met betrekking tot toegang dezelfde maatregelen.
- **Advies notitie:** Stel gemeenschappelijk risico's voor ketens vast bij risicoanalyses
- **Resultaat:** Analyse en rapportage hoe dit beleid in te richten. Onderzoeken of de huidige inrichting met het Convenant Digitale Onderwijsmiddelen en Privacy[6] 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. Door beleggen van werkpakket bij de EdustandaardIBP werkgroep is indirect aanhaking van leveranciers geborgd

### 2.1.3. 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 zorgt ervoor dat bepaalde doelgroepen kunnen beschikken over een authenticatiemiddel dat het vereiste betrouwbaarheidsniveau ondersteund.

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.

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

Dit in combinatie met het gebruik van een authenticatiemiddel van betrouwbaarheidsniveau substantieel maakt het mogelijk dat authenticatiediensten van onderwijsinstellingen betrouwbaarheidsniveau Substantieel 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. Op basis van de risicoanalyse zal dit Laag, Substantieel of Hoog zijn.
- **Onderzoeksvraag notitie:** Onderzoek hoe gebruik kan worden gemaakt van andere authenticatiemiddelen
- **Resultaat:** Voorstel welke authenticatiemiddelen bepaalde doelgroepen moeten kunnen gebruiken.
- **Belegd bij:** OCW / Deelnemers fase A

### 2.1.4. 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 en medewerkers die namens een organisatie gemachtigd zijn op een dienst af te nemen. Er zijn zo (per sector) meerdere doelgroepen waarvoor specifieke eisen gelden.

- **Doel:** Voor specifieke doelgroepen is toegang geregeld.
- **Advies notitie:** Stel binnen het onderwijsdomein een gemeenschappelijk beleid voor de belangrijkste doelgroepen op.
- **Resultaat:** Per sector en doelgroep is inzichtelijk welke verklaringen nodig zijn om toegang tot diensten te verkrijgen.
- **Belegd bij:** OCW / Deelnemers fase A

### 2.1.5. Beleid ten aanzien van attributen ten behoeve van toegang

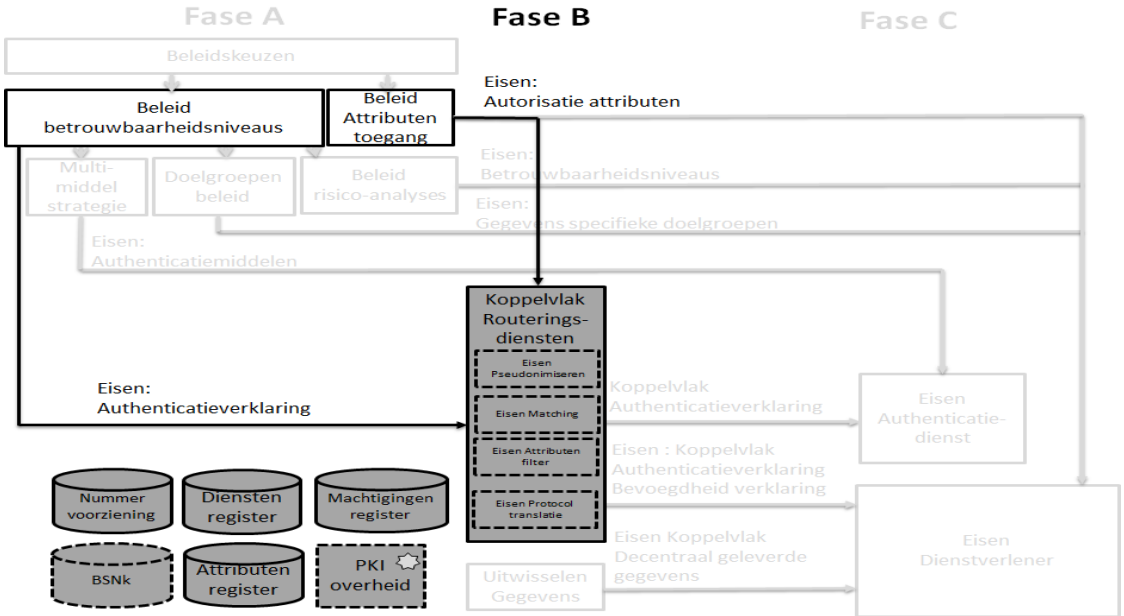
Het is wenselijk om een attributenbeleid ten behoeve van toegang (autorisatie) voor het onderwijsdomein op te stellen. Dit attributenbeleid is richtinggevend voor gegevens die bij toegang worden geleverd via de routeringsvoorziening(en) of via een directe koppeling.

- **Doel:** Dataminimalisatie, bij toegang worden alleen gegevens geleverd die voor autorisatie noodzakelijk zijn.
- **Advies notitie:** Stel attributenbeleid op voor autorisatie
- **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 / Deelnemers fase A

## 2.2. Projectresultaten fase B

In fase B 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. De regiegroep (en achterban) toetst tussentijdse de deliverables van fase B. In fase C wordt de impact hiervan in meer detail met decentrale rollen afgestemd. Het Toekomstbeeld Toegang van fase B geeft in concept weer wat centraal geregeld wordt.



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.
- **Belegd bij:** Kennisnet, SURF, DUO, Basispoort / Deelnemers fase B

### 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.
- **Belegd bij:** Kennisnet, SURF, DUO, Basispoort / Deelnemers fase B

### 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.
- **Onderzoeksvraag notitie:** Formuleer een beleid ten aanzien van identifiers en pseudoniemen
- **Resultaat:** Analyse van gebruikte authenticatiemiddelen door verschillende gebruikersgroepen en de identifiers en 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 identifiers en pseudoniemen en mogelijke overgangen. Het resultaat vormt een onderdeel van het Toekomstbeeld Toegang.
- **Belegd bij:** Kennisnet, SURF, DUO, Basispoort / Deelnemers fase B

### 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 (verticale machtiging). Bij

machtigen gaat het in principe om het (tijdelijk) kunnen overdragen van bevoegdheden en deze bevoegdheden moeten bij toegang gevalideerd kunnen worden.

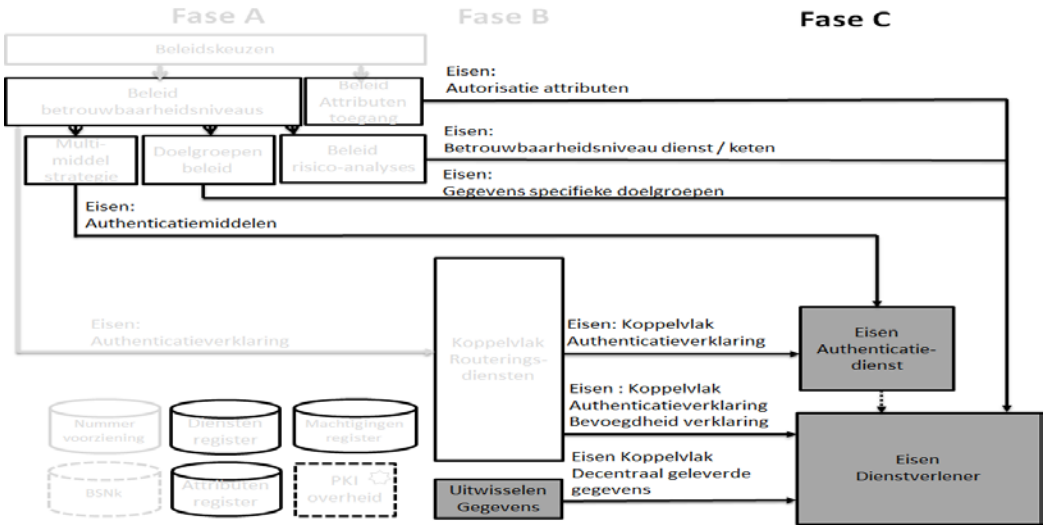
Een centraal (gefedereerd) register voor de registratie van machtigingen lijkt wenselijk. Hoe worden deze geleverd (via routeringsdienst of direct) en dienen deze bij een register geverifieerd te worden of worden deze in een digitale ondertekende verklaring geleverd? Komt er een centraal dienstenregister 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.
- **Onderzoeksvraag notitie:** Ontwikkel een visie op machtigen
- **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.
- **Belegd bij:** Kennisnet, SURF, DUO, Basispoort / Deelnemers fase B

### 2.3. Projectresultaten fase C

In fase C worden werkpakketten uitgevoerd die bij partijen kunnen worden belegd die decentrale rollen vervullen in het stelsel. De uitkomsten van de werkpakketten in fase B en de kaderstellende beleidskeuzen uit fase A worden in samenhang vertaald naar een tweede concept 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.
- **Belegd bij:** VDOD, GEU, CvTE / Deelnemers fase C

### 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.
- **Belegd bij:** VDOD, GEU / Deelnemers fase C

### 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.
- **Belegd bij:** VDOD, GEU, CvTE / Deelnemers fase C

### 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[7].

[7] https://fidoalliance.org/

- **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.
- **Belegd bij:** VDOD, GEU, CvTE / Deelnemers fase C

### 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[8]) 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.
- **Belegd bij:** VDOD, GEU, CvTE / Deelnemers fase C

### 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.

[8] 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.
- **Belegd bij:** VDOD, GEU, CvTE / Deelnemers fase C