Notitie Analyse IAA initiatieven

Van: **Edustandaard IAA-werkgroep**
Aan: **Edustandaard Architectuurraad**
Versie: **0.99**
Datum: **April 2018**

Inhoudsopgave

1 Inleiding

De digitalisering neemt toe, ook in het onderwijs worden steeds meer processen met digitale diensten ondersteund. We zien een toename van samenwerking tussen onderwijsinstellingen en van onderwijsdeelnemersmobiliteit. Bij dit laatste moeten onderwijsdeelnemers toegang krijgen tot informatie over relevante onderwijseenheden van een andere instelling, zich daarvoor kunnen aanmelden en toegang krijgen tot de betreffende digitale leeromgeving. Verder moet studievoortgangsinformatie gemakkelijk, veilig en betrouwbaar tussen onderwijsinstellingen uitgewisseld kunnen worden.

Dit alles heeft consequenties voor de uitwisseling van gegevens tussen partijen en de toegang tot diensten. In de huidige situatie verschilt de wijze van toegang per sector en is vaak ook afhankelijk van het proces. Het is zeer wenselijk dat onderwijsdeelnemers en onderwijspersoneel op een uniforme wijze toegang wordt geboden.

Als gevolg van de digitalisering zien we ook een toename in regelgeving. Er worden steeds hogere eisen gesteld aan het borgen van privacy. Een voorbeeld hiervan is de Europese Algemene Verordening Gegevensbescherming (AVG[1]). En ook de overheid onderkent de noodzaak van het regelen van toegang op een uniforme wijze. Als onderdeel van de Wet Digitale Overheid[2] (DO, voorheen GDI) komen authenticatiemiddelen voor burgers en bedrijven beschikbaar die voldoen aan de betrouwbaarheidsniveaus (laag, substantieel en hoog) van eIDAS[3].

[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/

Het betrouwbaarheidsniveau van het huidige authenticatiemiddel binnen het onderwijsdomein kan over het algemeen volgens eIDAS als laag geclassificeerd worden. Voor specifieke doelgroepen in combinatie met bepaalde diensten is dit te laag. Daarnaast zullen de eisen in de loop van de tijd strenger worden waardoor dit ook bij andere doelgroepen en diensten gaat spelen.

Binnen het onderwijsdomein zijn verschillende initiatieven rond Identificatie, Authenticatie en Autorisatie (IAA) gestart om een toekomstbeeld voor toegang op te stellen. De Edustandaard Standaardisatieraad heeft onderkend dat het belangrijk is dat deze toekomstbeelden op elkaar aansluiten. Daarom heeft de Standaardisatieraad een werkgroep ingesteld met als opdracht de toekomstbeelden te vergelijken, te onderzoeken waar overeenkomsten en verschillen zitten en aan te geven welke beleidskeuzes nodig zijn om de toekomstbeelden te harmoniseren. Deelnemers van de werkgroep waren vertegenwoordigers van OCW, DUO, SURF, saMBO-ICT, PO-Raad en VO-Raad, de GEU, de VDOD en Kennisnet/Edustandaard. De werkgroep is september 2017 gestart en levert het eindrapport in april 2018 op. De werkgroep heeft Toekomstperspectief toegang (Edu-K), Visie op IAA (SURFnet) en Wet Digitale Overheid geanalyseerd. Deze toekomstbeelden zijn redelijk globaal van karakter. Aanvullend is een aantal use cases (zie Bijlage A: Overzicht besproken use case) uit alle sectoren onderzocht om de wijze van toegang in de huidige situatie te onderzoeken. Dit verschaft een gedetailleerd beeld van de verschillen tussen sectoren en toepassingsgebieden. Bij de analyse van de toekomstbeelden en use cases is gelet op de volgende aandachtsgebieden:

1. Doelstelling
2. Centralisering
3. Identificatie en authenticatie
4. Autorisatie
5. Machtigen medewerker
6. Visie rond digitalisering

2 Bevindingen

De werkgroep heeft getoetst of de verschillende IAA-initiatieven op elkaar aansluiten en tevens onderzocht hoe deze zich verhouden met de huidige situatie. Hieronder wordt per aandachtsgebied beschreven wat de overeenkomsten en verschillen zijn:

1. **Doelstellingen zijn gelijk.**
   De initiatieven onderkennen de effecten van de digitalisering en eisen die er vanuit wetgeving wordt gesteld. De focus van de initiatieven ligt bij toegang waarbij ook privacy en beveiliging conform de actuele wet- en regelgeving belangrijke aandachtspunten zijn. De initiatieven zijn toekomstbeelden of richtinggevende kaders en hebben een redelijk abstract karakter.

2. **Verschillende keuzes rond centralisering.**
   De toekomstbeelden maken andere keuzes voor de mate van centralisering. *Toekomstperspectief Toegang* adviseert toe te werken naar één centrale toegangsdienst. Andere initiatieven hanteren voor toegang een decentraal model met een stelsel van toegangsdiensten.

3. **Er blijven verschillen rond identificatie en authenticatie.** De initiatieven bieden soms meerdere oplossingen voor hetzelfde vraagstuk en laten aan de andere kant een aantal vraagstukken onderbelicht.
    a. **De toekomstbeelden gaan allemaal uit van pseudonimisering.**
    Er is echter geen gedeeld beeld over de wijze waarop pseudonimisering vormgegeven moet worden. Dit kan op termijn interoperabiliteitsproblemen tot gevolg hebben en beperkt mogelijk het (her)gebruik van (centrale) voorzieningen.
    b. **Betrouwbaarheidsniveaus zijn niet gestandaardiseerd.**
    Dienstaanbieders zijn zelf verantwoordelijk voor het vaststellen van het vereiste betrouwbaarheidsniveau voor hun dienst. Om dit te bepalen kunnen zij gebruik maken van de handreiking betrouwbaarheidsniveaus van forumstandaardisatie[4] en de regelhulp tool[5]. Vervolgens moet er een keuze worden gemaakt welke toegangskanalen / stelsels het vereiste minimale betrouwbaarheidsniveau bieden. Het is dus van belang dat ook deze stelsels/ authenticatiemiddelen expliciet aangeven welk betrouwbaarheidsniveaus ondersteund worden. Verschillende stelsels binnen het onderwijs hanteren nog niet gestandaardiseerde betrouwbaarheidsniveaus conform de eIDAS verordening.
    c. **De te grote digitale sleutelbos wordt onderkend.**
    Een concrete oplossing om deze terug te dringen ontbreekt echter. Bij de digitale overheid is dit een belangrijk aandachtspunt en er wordt gewerkt aan een publiek en een privaat authenticatiemiddel voor burgers dat minimaal kan worden gebruikt bij alle overheidsdiensten. Een belangrijk kenmerk is dat deze authenticatiemiddelen minimaal het eIDAS-betrouwbaarheidsniveau substantieel ondersteunen. Binnen het onderwijsdomein is er momenteel geen keuze in authenticatiemiddelen, een authenticatiemiddel met betrouwbaarheidsniveau substantieel ontbreekt. Dit is wel wenselijk om met de steeds hogere eisen die aan toegang gesteld worden flexibel om te kunnen gaan. SURFconext en Entree Federatie maken gebruik van het door de onderwijsinstelling geleverde authenticatiemiddel. Het betrouwbaarheidsniveau is laag. Het niet beschikken over authenticatie middelen met verschillende betrouwbaarheidsniveaus zal tot problemen leiden als overgestapt moet worden naar betrouwbaarheidsniveau substantieel. Of als het verplicht wordt om Rijksbrede authenticatiemiddelen te gebruiken.

4. **Autorisatie-attributen zijn niet gestandaardiseerd.**
    De toegangsdiensten hanteren elk een andere set attributen voor autorisatie. Het *Toekomstperspectief Toegang* refereert naar het attributenbeleid[6] dat Edu-K heeft opgesteld. De focus van het attributenbeleid is echter beperkt tot processen van de ECK-keten. Voor standaardisatie van de attributen die bij toegang (autorisatie)

[4] https://www.forumstandaardisatie.nl/thema/handreiking-betrouwbaarheidsniveaus

[5] https://regelhulpenvoorbedrijven.nl/betrouwbaarheiddigitaledienstverlening/

[6] https://static1.squarespace.com/static/582171d81b631bd084b24eef/t/58ff22595016e163f206ce35/1493115481663/Attributenbeleid+ECKiD+v1.0.pdf

via de toegangsdiensten geleverd worden worden zouden ook andere processen moeten worden meegenomen, bijvoorbeeld de administratieve processen.

5. **Machtigingen worden onderkend, maar een concrete oplossing ontbreekt.**
   Binnen het onderwijs zijn er veel situaties waar sprake is van machtigen. Bijvoorbeeld bij verticaal machtigen waarbij een medewerker namens een onderwijsinstelling diensten kan afnemen van een dienstaanbieder. Een dienstaanbieder wil kunnen vaststellen of de medewerker bevoegd is om de dienst af te nemen. Het *Toekomstperspectief Toegang* refereert naar eHerkenning[7], maar onderkent niet in detail het machtigingsvraagstuk. Het is nu niet duidelijk of eHerkenning de gewenste oplossing is. BZK heeft een programma Machtigen gestart dat een toekomstbeeld voor machtigen gaat opstellen. Dit project gaat een projectstartarchitectuur opstellen voor een stelsel van voorzieningen die zowel horizontale als verticale machtigingen ondersteunen. Bij het toekomstbeeld van het onderwijsdomein zal aangegeven moeten worden op welke wijze aangesloten kan worden op dit stelsel.

6. **Een gemeenschappelijke visie op de gemeenschappelijke infrastructuur ontbreekt.**
   De eisen die aan de technische infrastructuur worden gesteld veranderen. Er zijn nieuwe functionele behoeften en de huidige standaarden voldoen in sommige situaties niet. Zo zien we bijvoorbeeld de behoefte aan een protocoltranslatie functie en de ondersteuning van de OpenIDconnect standaard.

   Bij toegang worden autorisatie-attributen geleverd en wordt er naar een minimale gestandaardiseerde set gestreefd. Tegelijkertijd zijn er nog attributen nodig voor procesondersteuning waardoor ze niet verdwijnen. Voor procesondersteuning kunnen technische heel andere keuzes gemaakt worden dan voor toegang.

   Er is een gemeenschappelijke visie nodig die aangeeft welke rollen de infrastructuur moet vervullen, welke standaarden hierbij gebruikt worden, wat het toepassingsgebied van standaarden is en of gegevens hierbij *point-to-point* worden geleverd of via een centrale dienst. Er is een migratiepad nodig om stapsgewijs naar de gewenste situatie te migreren.

[7] https://www.eherkenning.nl/

3 Adviezen en onderzoeksvragen

Dit rapport heeft als doel aan te geven welke beleidskeuzes gemaakt moeten worden om tot een gezamenlijk toekomstbeeld toegang te komen. Op basis van de bevindingen in hoofdstuk 2 is bepaald dat er 3 aandachtsgebieden zijn waar harmonisatie nodig is:

1. Harmonisatie van beoogde effecten van toegang.
   Voor het onderwijsdomein zal beleidsmatig vastgesteld moeten worden wat het beoogd effect van toegang is. Bijvoorbeeld welk betrouwbaarheidsniveau wordt geboden en welke bestuurlijke randvoorwaarden gelden voor verschaffen van toegang voor specifieke doelgroepen. De inrichting van gemeenschappelijke beleidskeuzes rond IAA vormen een belangrijke basis om tot de realisatie van harmonische oplossingsrichtingen te komen.
2. Definiëring rolverdeling binnen toegang.
   Verlenen van toegang vergt samenwerking tussen een groot aantal actoren. Een duidelijke rolverdeling (wie doet wat) is hierbij essentieel.
3. Definiëren functionaliteit technische infrastructuur.
   Voor uitvoering van de toegangsrollen wordt gebruik gemaakt van een technische infrastructuur. Het is wenselijk dat gedefinieerd wordt welke functionaliteiten de technische infrastructuur moet bieden en op welke wijze deze functionaliteiten de toegangsrollen ondersteunen.

Per aandachtsgebied wordt beschreven welke acties bij kunnen dragen aan harmonisatie. Hierbij wordt een verschil gemaakt tussen adviezen en onderzoeksvragen. Bij een advies wordt een voorstel gedaan voor een oplossingsrichting. Bij een onderzoeksvraag moet er nog gekozen worden tussen alternatieven, waarbij de consequenties nog onvoldoende duidelijk zijn.

3.1 Harmonisatie beoogde effecten toegang

Ketenpartners maken afspraken over de gewenste effecten van toegang.

3.1.1 **Beleid ten aanzien van betrouwbaarheidsniveau**

Ketenpartners maken samen afspraken over gewenst betrouwbaarheidsniveau. Zo is er het Convenant Digitale Onderwijsmiddelen en Privacy[8] dat de AVG vertaalt naar de onderwijspraktijk van het po, vo en mbo. Het bevat afspraken over het omgaan met persoonsgegevens bij het gebruik van digitale leermiddelen en toetsen. Aan de beveiligingsbijlage van het privacyconvenant is een verwijzing naar het certificeringsschema[9] toegevoegd. Dit certificeringsschema helpt leveranciers om hun producten te classificeren op de kenmerken: Betrouwbaarheid, Integriteit en Vertrouwelijkheid en geeft verder aan welke beveiligingsmaatregelen je bij iedere classificatie zou kunnen of zou moeten nemen. Dit bepaalt tevens het minimaal vereiste betrouwbaarheidsniveau bij toegang.

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

[9] https://www.edustandaard.nl/standaard_afspraken/certificeringsschema-informatiebeveiliging-en-privacy-rosa/certificeringsschema-informatiebeveiliging-en-privacy-rosa/

Adviezen:

- Volg eIDAS indeling voor betrouwbaarheidsniveaus. Maak hierbij gebruik van het certificeringsschema, de handreiking betrouwbaarheidsniveaus van Forum Standaardisatie[10] en de regelhulp tool[11].
- Stel gemeenschappelijk risico voor ketens vast bij risicoanalyses.
  Een risicoanalyse bepaalt welke maatregelen proportioneel zijn. Bij samenwerking in een keten zou het risico gelijk moeten zijn. En kan gezamenlijk een betrouwbaarheidsniveau voor een toepassingsgebied gekozen worden.

3.1.2 Beleid ten aanzien van doelgroepen

Stel binnen het onderwijsdomein een gemeenschappelijk beleid voor de belangrijkste doelgroepen op. 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 of mandatering mogelijk is en zo ja welke randvoorwaarden hiervoor gelden.

Maar denk ook aan beleid voor het regelen van toegang voor onderwijsdeelnemers die niet uit de EU afkomstig zijn.

3.2 Definiëring rollen binnen toegang

Uitvoeringsrollen

Bij de uitvoeringsrollen wordt onderscheid gemaakt tussen:

- dienstverlening;
- bieden van toegang functionaliteiten.

Dienstverlening

Dienstverleners bieden toegang aan gebruikers. Bij dienstverleners wordt onderscheid gemaakt tussen onderwijsinstellingen en leveranciers. Houd hierbij rekening met het verschil tussen uitvoering wettelijke taken en private diensten.
Onderwijsinstellingen voeren een wettelijke taak uit. Hierdoor is er sprake van doelbinding waardoor het per wet geregeld kan worden dat ze gerechtigd zijn om de identiteiten van onderwijsdeelnemers te kennen. Leveranciers voeren geen wettelijke taak uit. Zij mogen alleen persoonsgegevens verwerken als zij hiervoor een verwerkersovereenkomst sluiten.

Dienstverleners wisselen bij toegang berichten uit met andere actoren. De eisen die worden gesteld aan berichtuitwisseling veranderen. Er wordt meer en meer gebruik gemaakt van applicaties op verschillende (mobiele) devices waar de huidige standaarden voor toegang (zoals SAML) minder geschikt voor zijn. De REpresentational State Transfer (REST) [12] architectuurstijl is al jaren gemeen goed en de REST georiënteerde standaarden worden meer volwassen (zoals OpenID Connect) en zijn beter geschikt om toegang tot applicaties te ondersteunen. Verder zien we ook in bredere zin een verschuiving naar meer REST georiënteerde standaarden, zoals Oauth. Ontwikkelplatformen geven meer en meer prioriteit aan de ondersteuning van REST georiënteerde koppelingen.

[10] https://www.forumstandaardisatie.nl/thema/handreiking-betrouwbaarheidsniveaus

[11] https://regelhulpenvoorbedrijven.nl/betrouwbaarheiddigitaledienstverlening/

[12] http://www.restapitutorial.com/lessons/whatisrest.html

Toegangsfunctionaliteiten

Bij verschaffen toegang is er sprake van taakverdeling. Er kunnen verschillende rollen worden onderscheiden, die elk een specifieke functie vervullen: identificatie, authenticatie, gedelegeerde autorisatie en machtigen. Deze rollen kunnen belegd zijn bij verschillende actoren. Het resultaat van de uitvoering van een functie is een verklaring: identiteitsverklaring, authenticatieverklaring, autorisatieverklaring, machtigingsverklaring. Deze verklaring kan nodig zijn voor het uitvoeren van een andere functie. Authenticatie kan pas als een identiteit geregistreerd is. Voor gedelegeerde autorisatie is randvoorwaardelijk dat hiervoor al de identiteit is vastgesteld (met authenticatie). Omdat het niet waarschijnlijk is dat één actor alle functies uitvoert, moeten de verklaringen tussen actoren uitgewisseld kunnen worden. Dit kan rechtstreeks of via een routeringsfunctie.

3.2.1 **Identificatie**

Identificatie heeft als doel het vaststellen en delen van identiteiten. Voor de verduidelijking van onderstaande tekst worden hieronder een aantal begrippen toegelicht.

Identifier	Een label (meestal een string of tekst) waarmee je een entiteit (een persoon, object o.i.d.) aanduidt. Dit maakt het mogelijk om naar een entiteit te verwijzen. Zo'n entiteit heeft meestal meerdere identifiers die in verschillende contexten nuttig kunnen zijn.
Identiteit	De volledige maar dynamische set van alle attributen behorende bij een bepaalde entiteit die het mogelijk maakt betreffende entiteit van andere te onderscheiden. Elke entiteit heeft maar één identiteit. De identiteit behoort toe aan de entiteit. Bijvoorbeeld voor een Nederlands staatsburger zijn de BRP (incl. RNI) gegevens afgeleide attributen van de fysieke verschijningsvorm en het BSN de digitale identiteit waarmee hij/zij een afgeleide identiteitsverklaring kan krijgen (bijvoorbeeld reisdocument of uittreksel uit het bevolkingsregister).

Bij identificatie worden de volgende functies vervuld:

- Vaststellen identiteit
- Registreren digitale identiteit
- Matchen digitale identiteiten
- Leveren digitale identiteitsverklaring
- Pseudonimiseren

Vaststellen identiteit

Bij dit proces wordt de identiteit geverifieerd van een dienstafnemer waarvan toegang geregeld moet worden.

Registreren digitale identiteit

Bij dit proces worden de (geverifieerde) kenmerken geregistreerd. Eén van deze kenmerken is vaak een identifier waarmee de identiteit herleid kan worden. De wijze van het verifiëren van de identiteit en het registreren van de digitale identiteit zijn van invloed op het betrouwbaarheidsniveau.

Matchen digitale identiteiten

Er kunnen meerdere verstrekkers van digitale identiteiten zijn die elk een andere identifier verstrekken aan dezelfde persoon. Dit maakt matching noodzakelijk. Matching kan zowel op het niveau van de identiteit als identifier aan de orde zijn. Voorbeelden hiervan zijn:

- *Europese identiteiten matchen met BSN*
  Elk Europees land geeft eigen digitale identiteiten uit. In het kader van eIDAS is afgesproken dat bij een authenticatieverzoek vanuit een ander EU land op basis van een aantal persoonsgegevens en eventueel identifier gekeken wordt of de betreffende persoon al binnen Nederland een digitale identiteit heeft gekregen. In dit geval vindt koppeling plaats op basis van persoonskenmerken en/of de digitale identiteit van het betreffende land met het corresponderende BSN.
- *Onderwijsnummer matchen met BSN*
  Het kan voorkomen dat een onderwijsdeelnemer zonder een BSN een Onderwijsnummer als identifier heeft gekregen. Als deze persoon later alsnog een BSN krijgt wordt dit gekoppeld aan het corresponderende ON. Ook hier spelen een aantal persoonsgegevens een rol bij het matchingsproces.
- *Matchen ketenpseudoniemen van verschillende sectoren*
  Uitgegeven ketenpseudoniemen (identifiers) zijn persistent binnen een keten en sector. Bij overgang van de ene keten cq sector naar de andere is matching nodig. Hiervoor is nog geen standaard mechanisme en bepalen partijen onderling een oplossing.

Verstrekken digitale identiteitsverklaring

Een aantal van de geregistreerde kenmerken worden verstrekt aan andere rollen, bijvoorbeeld voor de provisioning van authenticatie. Dit proces ondersteunt ook andere fasen van de life cycle, bijvoorbeeld het kunnen doorgeven van wijzigingen of het verwijderen van de digitale identiteit.

Pseudonimiseren

Bij pseudonimisering wordt op basis van een algoritme een identiteit vertaald naar een pseudoniem met een beperkt werkingsgebied (bijvoorbeeld voor een organisatie of voor een keten/sector). De pseudonimisering kan bij meerdere rollen in de gemeenschappelijke infrastructuur uitgevoerd worden.

Onderzoeksvraag "Beleid ten aanzien van gebruik pseudoniemen"

- *Doel:* Formuleren beleid voor gebruik van pseudoniemen.
- *Resultaat:* Het onderzoek geeft uitsluitsel over het toepassingsgebied van pseudoniemen en geef aan hoe interoperabiliteit tussen pseudoniemen wordt geregeld.
- *Complicatie:* In huidige situatie worden verschillende pseudoniemen gebruikt. De volgende pseudoniemen worden gebruikt:
  - een domein pseudoniem (zoals het BSN);
  - een keten pseudoniem (zoals een Eck ID);
  - een specifiek pseudoniem;
  - een polymorf pseudoniem (versleuteld specifiek of domein pseudoniem).

Dit leidt tot problemen, bijvoorbeeld bij studenten- en medewerker mobiliteit. Zo kunnen in het ho en mbo studenten en medewerkers bij verschillende onderwijsinstellingen betrokken zijn. Er is een groeiend aantal studenten dat het studieprogramma in verschillende fasen samenstelt met vakken die ook door een andere dan de eigen instelling verzorgd worden.

3.2.2 **Authenticatie**

Authenticatie betreft het aantonen dat degene die zich identificeert ook daadwerkelijk degene is die zich als zodanig voorgeeft: ben je het ook echt? Authenticatie noemt men ook wel verificatie van de (digitale) identiteit. Bij authenticatie worden de volgende functies vervuld:

- Registreren authenticatiemiddel
- Gebruik authenticatiemiddel
- Leveren authenticatieverklaring

Registreren authenticatiemiddel

Er wordt een identifier (credential) en één of meerdere authenticatiemiddelen geregistreerd. Het authenticatiemiddel wordt aan de dienstafnemer uitgeleverd. De eIDAS-verordening kaders bepalen het betrouwbaarheidsniveau van het geregistreerde middel.

Gebruik authenticatiemiddel

Dit proces betreft de authenticatie van een dienstafnemer ten behoeve van toegang tot een digitale dienst. De dienstafnemer heeft het bezit en controle over één of meer authenticatiemiddelen om de digitale identiteit te claimen.

Verstrekken authenticatieverklaringen

Na de authenticatie van de dienstafnemer kan er een authenticatieverklaring geleverd worden aan de dienstaanbieder. Het uitwisselen van authenticatieverklaringen kan rechtstreeks of via een routeringsfunctie (van een toegangsdienst). In de huidige situatie wordt de authenticatie van een instelling gefedereerd. Wanneer het mogelijk moet worden om te kunnen kiezen tussen meerdere authenticatie-dienstverleners stelt dit eisen aan de standaardisatie van de authenticatieverklaring/identifiers.

Onderzoeksvraag "Onderzoek hoe gebruik kan worden gemaakt van andere middelen"

- *Doel:* Vaststellen hoe multi-middelen strategie gerealiseerd kan worden.
- *Motivatie:* De bestaande authenticatiemiddelen binnen het onderwijsdomein kunnen over het algemeen geclassificeerd worden op betrouwbaarheidsniveau laag (eIDAS). Er zijn nu processen waar gebruik wordt gemaakt van niveau midden. Dat is niet een betrouwbaarheidsniveau dat door eIDAS erkend wordt. Het kan zijn dat na analyse hier niet niveau midden nodig is, maar niveau substantieel. Verder kan het zijn dat bij processen waar nu laag gebruikt wordt het op termijn ook nodig zal zijn om substantieel te gebruiken. Daarom moet beleid worden geformuleerd voor de wijze waarop betrouwbaarheidsniveau substantieel ondersteund kan worden. Op korte termijn voor vervanging van DigiD midden en op langere termijn waarschijnlijk ook voor DigiD laag. Hierbij zal ook onderzocht moeten worden of het mogelijk en/of wenselijk is om aan te sluiten bij authenticatiemiddelen die elders worden gebruikt

(bijvoorbeeld iDIN, Idensys, eHerkenning of een sectorspecifieke authenticatiedienst). Bij het onderzoek naar andere middelen moet ook het perspectief van de gebruiker meegenomen worden. De te grote digitale sleutelbos is niet alleen vervelend voor de gebruiker maar leidt ook tot onveiligheid, toepassen van makkelijk te onthouden wachtwoorden of deze worden onveilig beheerd. Een gebruiker moet een beperkte digitale sleutelbos hebben die meerdere betrouwbaarheidsniveaus ondersteund.

- *Resultaat:* Architectuurkaders die multi-middelen strategie mogelijk maken.

3.2.3 **Autorisatie**

Autorisatie wordt gebruikt om op basis van de rol van een persoon te bepalen welke rechten deze persoon krijgt bij toegang. Voor autorisatie is berichtuitwisseling nodig. Enerzijds voor het uitwisselen van attributen die nodig zijn om een persoon te kunnen autoriseren. Anderzijds is het mogelijk om autorisatie te delegeren waarbij een verklaring wordt gestuurd dat een gebruiker geautoriseerd is om de gevraagde dienst af te nemen.

Uitwisselen autorisatie-attributen

Voor het autorisatieprofiel worden attributen uitgewisseld om aan te geven voor welke rollen wordt geautoriseerd. In de huidige situatie hanteren de toegangsdiensten ieder een andere set attributen voor autorisatie.

Advies: stel attributenbeleid op voor autorisatie

Het *Toekomstperspectief Toegang* refereert naar het attributenbeleid dat Edu-K heeft opgesteld. De focus van het attributenbeleid is echter beperkt tot processen van de ECK keten, zoals bestellen, leveren, gebruik van en toegang tot digitaal leermateriaal en het uitwisselen van leer- en toetsresultaten. Het is wenselijk om een sector-overschrijdend attributenbeleid ten behoeve van toegang (autorisatie) op te stellen dat bruikbaar is voor alle processen.

De autorisatie-attributen worden uitgewisseld via de routeringsfunctie van de gemeenschappelijke infrastructuur. Harmonisatie van de attributenset is een randvoorwaarde voor harmonisatie van de toegangsdiensten.

Verstrekken autorisatieverklaringen

Autorisatieverklaringen kunnen gebruikt worden in situaties waarbij een systeem over gegevens uit een externe bron wil beschikken zonder de noodzaak van de uitwisseling van persoonsgegevens of identiteitsinformatie. Een standaard die hierin ondersteuning biedt is Oauth[13]. De autorisatieverklaringen kunnen via een directe koppeling of via een routeringsfunctie worden uitgewisseld, maar deze standaard veronderstelt in principe een point-to-point koppelingen tussen systemen (client en resource server). Harmonisatie van de autorisatieverklaringen is een randvoorwaarde voor harmonisatie van de federaties en directe koppelingen.

[13] https://tools.ietf.org/html/rfc6749

3.2.4 **Machtigen**

Een persoon (natuurlijk of niet-natuurlijk) machtigt een andere persoon namens hem diensten af te nemen.

Onderzoeksvraag "ontwikkel een visie op machtigen"

- *Doel:* bepalen welke vorm van machtigen ondersteunt moet worden en geef hiervoor architectuurkaders.
- *Motivatie:* organisaties die persoonsgegevens verwerken (verwerkers), of namens hen laten verwerken door andere organisaties (subverwerkers), moeten inzicht hebben in welke persoonsgegevens verwerkt worden en waarom. Hiermee wordt het van belang dat ook bij toegang kan worden vastgesteld namens wie (welke organisatie) een dienst afgenomen wordt. Hiermee is er ook binnen het onderwijsdomein behoefte om personen en bedrijven in bepaalde situaties te machtigen om namens een bepaald bedrijf te handelen. Het gaat hierbij in principe om het (tijdelijk) overdragen van bevoegdheden en deze bevoegdheden moeten bij toegang gevalideerd kunnen worden.
- *Resultaat:* architectuurkaders die een machtingsstelsel mogelijk maken.
- *Complicatie:* Er zijn veel verschillende vormen van machtigen. Het is wenselijk om aan te sluiten bij Rijksbrede ontwikkelingen, maar daar wordt nog gewerkt aan een toekomstbeeld. En de eisen die gesteld worden aan machtigen kunnen per domein sterk verschillen.

3.3 Definiëren functionaliteit technische infrastructuur

De technische infrastructuur ondersteunt de functies van de verschillende toegangsrollen met als doel om een gebruiker in staat te stellen een dienst af te nemen waarbij voldaan kan worden aan de eisen die de dienstaanbieder bij toegang stelt.

Mede door de digitalisering zien we de eisen die aan de technische infrastructuur worden gesteld veranderen. We zien een toename van het gebruik van applicaties op mobile devices en de REST georiënteerde standaarden die hierbij ondersteuning bieden. Gegevens worden niet alleen uitgewisseld bij toegang of het gebruik van een dienst, maar ook in veel andere situaties. De uitwisseling vindt in sommige gevallen via directe koppelingen plaats en in andere via centrale voorzieningen (hubs).

Advies: stel een gedeeld toekomstbeeld voor de technische infrastructuur op en zorg dat deze actueel blijft.

Zorg ervoor dat er een gedeeld toekomstbeeld wordt opgesteld voor de technische infrastructuur op basis van de gewenste functionaliteit. Dit toekomstbeeld moet blijven aansluiten bij veranderende eisen van de omgeving. Borg daarom de verantwoordelijkheid voor het actueel houden van het toekomstbeeld.

In dit toekomstbeeld worden de adviezen meegenomen die de werkgroep doet ten aanzien van de infrastructuur:

1. Protocoltranslatie bij verstrekken authenticatieverklaringen.
2. Standaardisatie betrouwbaarheidsniveaus bij verstrekken authenticatieverklaringen.
3. Toepassingsgebieden standaarden en decentrale en centrale gegevensuitwisseling.

3.3.1 Protocoltranslatie bij verstrekken authenticatieverklaringen

Advies: standaardiseer OpenID Connect profielen

Conform het *Toekomstperspectief Toegang* wordt geadviseerd om bij de Toegangsdiensten OpenID Connect[14] te ondersteunen. De toegangsdiensten kunnen op basis van een protocoltranslatie de SAML-verklaring van de authenticatiedienst van de onderwijsinstelling omzetten naar OpenID Connect.

Advies: implementeer standaard OpenID Connect profiel bij toegangsdiensten.

Bij de ondersteuning van OpenID Connect is het van belang dat er bij de toegangsdiensten waar mogelijk dezelfde keuzes maken. Zorg dat de huidige toegangsdiensten binnen het onderwijsdomein zoals Entree Federatie en SURFconext, zoveel mogelijk hetzelfde profiel ondersteunen.

3.3.2 Standaardisatie betrouwbaarheidsniveaus bij verstrekken authenticatieverklaringen

Het standaardiseren van de betrouwbaarheidsniveaus is een randvoorwaarde voor de standaardisatie van de infrastructuur.

3.3.3 Toepassingsgebieden standaarden en decentrale en centrale gegevensuitwisseling

Bij de standaarden zijn er vaak alternatieven mogelijk. Criteria die hierbij een rol spelen zijn:

- *Voorkeur voor WUS of REST georiënteerde standaarden*

Bij toegang kan gebruik worden gekozen worden tussen bestaande standaarden (zoals SAML) en REST georiënteerde standaarden (zoals OpenID Connect en Oauth).

- *Gegevens nodig voor toegang of procesondersteuning*

Voor toegang worden andere standaarden gebruikt dan voor procesondersteuning. In de huidige situatie worden de federaties ook gebruikt voor gegevens die nodig zijn voor procesondersteuning. Dit is niet wenselijk.

- *Voorkeur voor centrale routeringsfunctie of directe koppeling*

Bij een centrale routeringsfunctie worden ander standaarden gebruikt dan bij directe koppelingen. We zien toenemende belangstelling voor voorzieningen die decentrale gegevensuitwisseling ondersteunen zoals een serviceregister.

Het is wenselijk inzicht te hebben wat gewenste werkings- en toepassingsgebieden van deze standaarden zijn.

Advies: ontwikkel als onderdeel van het toekomstbeeld ook een referentiearchitectuur met werkings- en toepassingsgebieden van de verschillende standaarden voor gegevensuitwisseling.

[14] http://openid.net/connect/

Bijlage A: Overzicht besproken use cases

1. **Studentmobiliteit HO**
   Toegang tot digitale diensten verloopt via de authenticatiedienst van de onderwijsinstelling. Studenten in het HO stellen in verschillende fasen het studieprogramma samen met vakken die ook door een andere dan de eigen instelling verzorgd worden. Instellingen zijn daardoor steeds meer van elkaar afhankelijk voor een optimale IT-ondersteuning van deze studentmobiliteit. Er zijn hierbij problemen door meervoudige authenticatiemiddelen en identifiers met als gevolg dat studenten moeizaam toegang krijgen tot noodzakelijke onderwijsvoorzieningen. Het heeft ook een administratief moeizaam proces tot gevolg bij het uitwisselen van studievoortgangsinformatie tussen onderwijsinstellingen.

2. **Toegang Studielink HO**
   Studielink ondersteund twee toegangskanalen, één via DigiD en één via de authenticatiedienst (geïntegreerd in applicatie) van Studielink. DigiD wordt gebruikt door studenten met een DigiD en de authenticatiedienst van Studielink wordt gebruikt door overige studenten en medewerkers. Momenteel loopt er een pilot met een derde toegangskanaal. Deze bestaat uit de authenticatiedienst van de onderwijsinstelling en SURFconext en zal worden gebruikt om medewerkers toegang te geven. Op termijn komt er ook een toegangskanaal voor EU studenten die dan hun eigen Nationaal authenticatiemiddel kunnen gebruiken.

3. **Deelnemermobiliteit PO**
   Toegang tot digitale diensten verloopt via de authenticatiedienst van de onderwijsinstelling. De dienstaanbieder krijgt voor een bepaalde gebruiker bij toegang verschillende identiteiten en attributen geleverd krijgt afhankelijk van het gekozen toegangskanaal (authenticatiedienst-toegangsdienst). Binnen de sector zijn er verschillende partijen die gegevens kunnen en mogen delen, maar het blijkt lastig om vast te stellen dat deze gegevens betrekking hebben op een bepaald persoon. Een dergelijk matchingsvraagstuk zien we ook bij use case 1. Bij processen/diensten waarbij niet het BSN of een ander gedeelde identifier gebruikt kan worden, wordt vaak een ad hoc oplossing toegepast, zoals het matchen op basis van persoonsgegevens.

4. **Bestellen en gebruik digitale leermiddelen VO/MBO**
   Toegang tot digitale diensten verloopt via de authenticatiedienst van de onderwijsinstelling en Entree Federatie of SURFConext. Met name in het VO speelt de identiteit van de onderwijsinstelling een belangrijke rol, omdat deze betrokken is bij het bestelproces. In het MBO is het de student zelf die de bestelling uitvoert. Ook bij deze use case zijn er meerdere partijen die gegevens uitwisselen over een

bepaald persoon. De oplossingsrichting die hier gekozen is dat meerdere partijen dezelfde identifier van de onderwijsdeelnemer gebruiken. Met het gebruik van deze keten identifier (ECK iD) kan de uitwisseling van overige (persoons)gegevens ten behoeve van de identiteitsbepaling geminimaliseerd worden. Er een aantal scenario's waar er alsnog een matchingsvraagstuk lijkt te ontstaan doordat het ECK iD een beperkt werkingsgebied heeft. Dit is bijvoorbeeld het geval wanneer een leerling de overstap maakt van vmbo naar mbo en hierdoor er bij toegang een nieuw ECK iD geleverd wordt. Dit levert problemen op bij doorlopende leerlijnen, die door steeds meer leermiddelen wordt ondersteund. Analyse van de use case maakt verder duidelijk dat de attributen van de toegangsdiensten Entree Federatie en SURFconext verschillend zijn. Er worden verschillende attribuutnamen gebruikt, of als deze dezelfde naam hebben is niet duidelijk of het gegeven van dezelfde bron afkomstig is.

5. **DUO Zakelijk portaal**
   DUO beheert de identiteiten en autorisaties van al haar zakelijke klanten, waarmee zij toegang kunnen krijgen tot de digitale diensten die DUO aanbiedt. De dienstafnemers zijn medewerkers van onderwijsinstellingen die namens een bevoegd gezag DUO diensten afnemen. DUO is momenteel intern aan het onderzoeken hoe op termijn toegang voor externen ingericht kan worden. De vraagstukken die hierbij spelen zijn op basis van welke gegevens identificatie kan plaatsvinden en hoe autorisaties ingericht gaan worden.

6. **H2M2M (autorisatie en machtiging medewerker)**
   Deze use case staat beschreven in het streefbeeld H2M2M en is gericht op het uitwisselen van vertrouwelijke (persoons)gegevens en de noodzaak om de handelende medewerker te kunnen machtigen en autoriseren. De gegevens van leerlingen, medewerkers of organisaties worden bij vele diensten binnen het onderwijs gebruikt. Hierbij wordt veel gebruik gemaakt van SaaS diensten, bijvoorbeeld studentadministratiesystemen (LAS/SIS). Er zijn zo vele digitale diensten die een medewerker (van onderwijsinstelling of andere organisatie binnen de onderwijssector) moet kunnen afnemen. De dienstaanbieders hebben vaak een eigen toegangskanaal (authenticatiedienst) ingericht en geven hiervoor ook eigen authenticatiemiddelen uit. De dienstafnemer heeft zo vele authenticatiemiddelen en moet bijhouden bij welke dienst wat gebruikt moet worden. Afhankelijk van de frequentie waarmee de dienst wordt afgenomen zijn dit ook vaak niet persoonsgebonden middelen, maar wordt het authenticatiemiddel gedeeld tussen vele medewerkers en is het proces rond beheer en gebruik ad hoc ingericht wat het beoogde betrouwbaarheidsniveau ondermijnt. Er moet verder ook betrouwbaar aangetoond kunnen worden dat de dienstafnemer bevoegd is om namens een bepaalde organisatie te handelen (verticale machtiging). Een generieke oplossing voor een beperkte digitale sleutelbos met ondersteuning van betrouwbaarheidsniveau substantieel en het kunnen registreren en leveren van machtigingen ontbreken.