Conceptversie verslag werkgroep IAA

Aanwezig:	Tine de Mik (Studielink), Frits Bouma (DUO), Jacob Hop (Aventus, MBO), Antoinette Erdmann (Dotcomschool, VDOD), Sir Bakx (Surfmarket), Bram Gaakeer (OCW, voorzitter), Erwin Reinhoud (Kennisnet, Bureau Edustandaard).
Afwezig:	Roel Rexwinkel (SURFnet), Brian Dommisse (Kennisnet, PO/VO raad), Freek Nabuurs (Cito)
Agendalid:	Pieter Ruempol (GEU)

Datum en locatie
30 november 2017, 10:00-12:00 uur, SURF-net , Utrecht

Agenda

1. **Opening, mededelingen, vaststellen agenda**
2. **Doornemen verslag van 2 november 2017 en actielijst**
3. **Use cases**
    a. **UC2: Aanvullingen toegang tot Studielink**
    b. **UC4: Bestellen / Toegang / Gebruik leermiddelen (VO en MBO)**
    c. **UC5: Aanvullingen Zakelijk portaal DUO**
4. **Kernpunten en positionering in het landschap.**
5. **Vervolg afspraken inplannen**
6. **Rondvraag**
7. **Afsluiting**

1. Opening, mededelingen, vaststellen agenda

Jacob Hop is een nieuwe deelnemer aan het overleg en zal Jan Bartling vervangen.

De agenda wordt zonder wijzigingen vastgesteld.

2. Doornemen verslag en actielijst van 2 november 2017

De beschrijving van use case 1 stelt dat de niet bekostigde student zich direct tot de Onderwijsinstelling richt voor de aanmelding en inschrijving. Dit probleem is dus gerelateerd aan het aanmeld- en inschrijfproces en de communicatie naar de niet bekostigde student. Het verslag van 2 november wordt op dit punt aangepast.

Er wordt verder opgemerkt dat het begrip publieke dienst nog steeds onduidelijk is. Er wordt besloten dat of iets een publieke dienst is onderdeel blijft van de lijst met criteria en onderdeel van de landschapsplaat. De deelnemers die verantwoordelijk zijn voor een bepaalde use case geven hier voorlopig zelf invulling aan. Het onderkennen van publieke en private diensten is belangrijk. We gaan mede vanwege de ontwikkelingen rond GDI nu nog niet een al te strikte definitie hanteren voor een publieke dienst. Het verslag van 2 november wordt op dit punt aangepast.

Het is niet geheel duidelijk of de use case de huidige of toekomstige situatie moeten beschrijven. Het idee was om de huidige situatie te beschrijven in de use case. Op basis hiervan kan dan aangegeven worden wat de impact van de verschillende initiatieven/toekomstvisies zijn. Bij use case 4 wordt wel alvast het ECKiD meegenomen omdat de toepassing hiervan binnenkort al gaat plaatsvinden.

In het verslag staat bij use case 2 dat niet alle HO-opleidingen zijn aangesloten op Studielink, dit moet worden gewijzigd in: Alle bekostigde opleidingen zijn aangesloten op Studielink.

3. Toelichting use cases

Er wordt besloten om agendapunten 3 en 4 te combineren.

3.1. Use case 2: Studielink

Toegangskanalen bij aanmelden

Er worden nu twee toegangskanalen onderkend, 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. Afhankelijk van hoe zaken rond eIDAS ingericht gaan worden is er in de toekomst ook een toegangskanaal voor EU studenten die dan hun eigen Nationaal authenticatiemiddel kunnen gebruiken.

Inschrijvingsproces

Nadat de student zich bij Studielink heeft aangemeld, ontvangt de betreffende onderwijsinstelling de gegevens van Studielink. Zoals in het vorige verslag beschreven verloopt het inschrijvingsproces verder bij de onderwijsinstelling zelf. Als er gebruik is gemaakt van een Studielink account (login), wordt er vanuit Studielink geen BSN meegegeven en bevat het verificatiebericht naar DUO het Studielinknummer. Het is nu onduidelijk welke gegevens worden gebruikt om te matchen als er geen BSN is. Dit zal bij het volgende overleg worden toegelicht (actiepunt #9). Verder is er zoals eerder beschreven voor de niet bekostigde student geen BSN en mogelijk ook geen Studielinknummer.

Identiteiten en koppelpunten

De identiteit die DUO levert is het PGN. Deze is gelijk aan het BSN in het verificatiebericht als deze hierin opgenomen was. Op verschillende locaties (Onderwijsinstelling, DUO en Studielink) worden verschillende identiteiten aan elkaar gekoppeld (o.a. BSN/PGN en Studielinknummer). Voor onze analyse vinden we het relevant om inzichtelijk te hebben welke identiteiten er binnen een bepaalde sector of overgang toegepast worden en wat het werkingsgebied hiervan is. Bij het volgend overleg zullen we derhalve meer aandacht besteden aan welke identiteit(en) er zijn en waar overgangen/koppelpunten zijn (actiepunt #10).

Er wordt opgemerkt dat we de term identiteit gebruiken, maar dat het niet een identiteit betreft, het studielinknummer of het specifiek pseudoniem dat bij het toegangsproces aan een bepaalde dienst geleverd wordt zijn geen identiteiten. We zullen hiervoor een andere term moeten gebruiken en de definitie hiervan opnemen in de begrippenlijst. (actiepunt #11).

De volgende aandachtspunten zijn bij deze use case naar voren gekomen:

1. Onderwijsinstellingen moeten na aanmelding bij Studielink alsnog een verificatie uitvoeren. Met name rond EU studenten is dit een extra administratieve last.
2. Hoe om te gaan met de situatie dat een bepaald persoon in verschillende rollen handelt en dat het IAA-stelsel hier flexibel mee om moeten kunnen gaan zodat de juiste gegevens voor de autorisatievraag geleverd kunnen worden. Ook betrouwbaarheid van het attribuut ‘rol’ is een aandachtspunt.
3. Medewerkers van een onderwijsinstelling hebben een account bij Studielink (authenticatiedienst). Er loopt een pilot om medewerkers toegang te geven via authenticatiedienst van onderwijsinstelling en SURFconext.

3.2. Use case 3 en 4: Bestellen en gebruik leermiddelen (ECK keten) en overige diensten binnen VO/MBO

Bij deze use case spelen de toegangsdiensten SURFconext en Entree Federatie een belangrijke rol. SURFconext wordt in het MBO en HO toegepast en Entree Federatie in het PO, VO en MBO. Dat beide in het MBO worden gebruikt is op zich geen probleem omdat beide in het MBO een eigen werkingsgebied hebben, Entree Federatie wordt met name gebruikt voor toegang tot diensten in de ECK keten, SURFconext ondersteund toegang tot cloud diensten. Wel is het wenselijk dat deze toegangsdiensten op een aantal punten standaardiseren.

Binnen de ECK keten is het ECKiD een belangrijke identiteit. Het ECKiD is uniek binnen een onderwijssector (PO, VO of MBO) en dus onafhankelijk van de onderwijsinstelling die de leerling/student identificeert en authenticeert. Het ECKiD voorkomt dat partijen in de ECK keten op basis van persoonsgegevens moeten

matchen. Het ECKiD wordt ook beschreven in het Toekomstperspectief toegang en omdat het ECKiD binnenkort ook toegepast gaat worden, is deze al in de beschrijving van de huidige situatie meegenomen.

Wat binnen deze use case als probleem wordt ervaren is dat de door de toegangsdiensten geleverde attributen niet gestandaardiseerd zijn. Voor een aantal attributen worden er verschillende attribuutnamen gebruikt. En als dezelfde attribuutnamen gebruikt worden is niet duidelijk of het gegeven van dezelfde bron afkomstig is. Tijdens de bespreking is er niet duidelijk welke attributen Entree Federatie[1] en SURFconext[2] leveren. Dit wordt uitgezocht en bij volgend overleg toegelicht(Actie #12). Hiermee kan inzichtelijk worden gemaakt welke attributen er bij toegang relevant zijn en welke later, bij gebruik (ondersteuning bedrijfsproces), relevant kunnen zijn. Het Toekomstperspectief toegang stelt voor om ook andere standaarden dan SAML te gebruiken voor het leveren van attributen na toegang (levering gegevens bij het gebruik van een dienst). Ook het attributenbeleid[3] kan op dit punt aanvullende informatie verschaffen.

Het is niet duidelijk of SURFconext een specifiek pseudoniem aan dienstaanbieders levert dat is afgeleid van het subject in de verklaring van de authenticatiedienst van de onderwijsinstelling. Ook dit punt moet onderzocht worden omdat het inzicht geeft in de afhankelijkheid en overgang van identiteiten, zie ook eerder actiepunt #10. Dit geldt tevens voor Entree Federatie.(actie #13)

Binnen de ECK keten in het VO bestelt de onderwijsinstelling vaak in bulk bij een distributeur. Er worden hierbij twee belangrijke varianten onderkend. Bij de eerste variant, een intern boekenfonds (IBF), levert de onderwijsinstelling door middel van een voucher. De leerling of docent wordt op basis hiervan bij het eerste gebruik geautoriseerd. De levering van het ECKiD bij toegang zorgt er voor dat de leerling of docent ook een volgende keer het product kan gebruiken conform licentievoorwaarden. Bij de tweede variant, een extern boekenfonds (EBF), communiceert de school naar de leerlingen en docenten bij welk bestelportaal leer- en docentenmateriaal gereserveerd is. De leerling of docent geeft bij het bestelportaal de onderwijsinstelling en opleiding aan en deze gegevens worden vanuit de toegangsdienst ook als attribuut geleverd. Op basis hiervan wordt de leerling of docent bij het eerste gebruik geautoriseerd. Het is dus met name bij het EBF-proces dat in de keten de identiteit van de onderwijsinstelling van belang is. Binnen de onderwijssector worden er voor onderwijsinstellingen en verbonden entiteiten verschillende identificerende kenmerken gebruikt. Dit kan het KvK-nummer of het BRIN zijn, maar ook een identiteit binnen een eigen (keten) registratie.

Naast dat ouders vaak toegang hebben tot diensten als een leerlingvolgsysteem, spelen zij vaak ook een rol bij het EBF-bestelproces in het VO. Welke rol zij hierin spelen en hoe toegang geregeld is varieert. In het MBO bestelt de student zelf bij de distributeur of uitgever en heeft (vaak direct) toegang tot het aangeschafte digitaal product.

De volgende aandachtspunten zijn bij deze use case naar voren gekomen:

1. Het betrouwbaarheidsniveaus zijn niet gestandaardiseerd - diensten kunnen niet een minimaal vereist betrouwbaarheidsniveau aangeven.
2. Geen standaardisatie van het koppelvlak tussen authenticatiedienst onderwijsinstelling en toegangsdiensten en koppelvlak tussen de toegangsdiensten en dienstaanbieders.
3. Docenten / studenten betrokken bij meerdere scholen hebben een middel per school. Binnen de ECK keten met toepassing van het ECKiD levert dat voor de dienstaanbieder geen probleem op.
4. In het MBO wordt meer en meer een betrouwbaar middel aan de authenticatiedienst van de school gekoppeld.
5. Ouders krijgen authenticatiemiddel per dienst of mogelijk een middel van school.

3.3. Use case 5 en 6: Het zakelijk portaal van DUO en overige diensten voor medewerker (H2M2M)

DUO levert niet alleen diensten binnen de onderwijssector, maar ook in de zorgsector en kinderopvang. Deze laatste twee zijn voor de IAA analyse niet direct relevant, maar speelt bij DUO wel een rol hoe om te gaan met toegang tot digitale diensten.

[1] https://developers.wiki.kennisnet.nl/index.php?title=KNF:Attributen_overzicht_voor_Service_Providers
[2] https://wiki.surfnet.nl/display/surfconextdev/Attributes+in+SURFconext
[3] https://static1.squarespace.com/static/582171d81b631bd084b24eef/t/58ff22595016e163f206ce35/1493115481663/Attributenbeleid+ECKiD+v1.0.pdf

Achter het zakelijk portaal zitten verschillende diensten waarbij voor elk afzonderlijke autorisaties gelden. Bij de registratie van een dienstafnemer worden een aantal gegevens verwerkt, zoals het BRIN van de onderwijsinstelling. Deze gegevens zijn door de onderwijsinstelling aangeleverd en ondertekend door het bevoegd gezag. Na registratie wordt er voor de dienstafnemer een ZP-account gecreëerd met o.a. persoonsgegevens, een user ID en toegekende rollen. De rollen worden gebruikt voor de autorisatie van de dienstafnemer. De mogelijke rollen worden gedefinieerd door DUO. Na koppeling van het token wordt deze met gebruikersnaam en wachtwoord aangetekend verstuurd naar de onderwijsinstelling van de dienstafnemer. Vaak wordt een applicatiebeheerder als eerste geregistreerd en zal deze daarna de aanvragen en autorisaties voor overige medewerkers regelen. De applicatiebeheerder is verantwoordelijk voor de uitgifte van het token aan de medewerker. Een belangrijk persoonsgegeven t.b.v. de communicatie naar de dienstafnemer is het emailadres.

In 2018 wordt onderzocht hoe eHerkenning ingezet kan worden voor toegang voor medewerkers van onderwijsinstellingen. De authenticatiediensten binnen eHerkenning hebben hun eigen registratieproces, dit heeft dus impact op de gegevens die geregistreerd en ontsloten kunnen worden. Een belangrijk onderdeel hiervan is de registratie van een machtiging. Binnen de overheid lopen er verschillende trajecten die aandacht aan machtigingen besteden. Ook de werkgroep moet een duidelijk beeld hebben bij wat gewenst is en wat er in de initiatieven/visies geboden wordt.

De volgende aandachtspunten zijn bij deze use case naar voren gekomen:

1. Geen generiek toegangskanaal voor medewerkers voor vele diensten binnen het onderwijs die zij in hun rol afnemen. Verschillende dienstaanbieders leveren de dienstafnemer vaak een eigen authenticatiemiddel (onnodige groei van sleutelbos).
2. Geen eenduidig beeld bij eisen rond een machtiging (bevoegdheid om namens een bepaalde organisatie een bepaalde dienst af te nemen), het registratieproces hiervan en hoe deze ontsloten kunnen worden.
3. Er wordt in verschillende trajecten onderzocht of en hoe eHerkenning als een generiek toegangskanaal voor medewerkers kan worden gebruikt. Mocht dit technische wenselijk zijn, is er nog de vraag hoe medewerkers over een eHerkenningsmiddel kunnen gaan beschikken.

4. Afsluiting

Met de huidige informatie en wat nog op basis van uitstaande acties beschikbaar komt willen we na het komend overleg meer inzicht krijgen in het volgende:

- Welke identiteiten zijn er, waar worden zij gebruikt en waar worden zij mogelijk aan elkaar gekoppeld
- Welke attributen worden er gebruikt en welke zijn mogelijk relevant voor autorisaties
- Welke eisen stellen we aan machtigingen (bevoegdheid medewerker om namens een organisatie te handelen / verticale machtiging).
- Welke koppelvlakken zijn er en waar zien we mogelijk een noodzaak voor transformaties.

Het volgende overleg is op 25 januari 2018 van 13:00 tot 15:00 uur.

5. Actielijst

#	Omschrijving	Status	Einddatum	Actie-houder	Prio
01	Voor uitwerking use case 4b moet nog bepaald worden wie VO use case inbrengt	Afgehandeld, Erwin zal use case 4b uitwerken	Begin oktober	Voorzitter/BES	1
02	Relevant materiaal op internet plaatsen	Afgehandeld	Begin oktober	BES	1

03	Use case 1 (o.b.v. patroon criteria) studentmobiliteit - de niet bekostigde internationale student (HO)	Afgehandeld	2 nov. 2017	Sir en Roel	2
04	Use case 2 (o.b.v. patroon criteria) toegang studielink - bekostigde student en onderwijsinstellingsmedewerker	Afgehandeld	30 nov. 2017	Tine	1
05	Use case 3 (o.b.v. patroon criteria) studentmobiliteit – binnen en buiten sector (bijv leer- en toetsomgeving & volgsystem, opleiding bij meerdere instellingen/sectoren)	Afgehandeld	2 nov. 2017	Antoinette en Freek	2
06a	Use case 4a (o.b.v. patroon criteria) bestellen en gebruik leermiddelen en diensten, met gebruik van Entree Federatie /SURFconext (MBO).	Afgehandeld	30 nov. 2017	Jacob Hop	1
06b	Use case 4b (o.b.v. patroon criteria) bestellen en gebruik leermiddelen en diensten (ECK keten), met gebruik van Entree Federatie(VO)	Afgehandeld	30 nov. 2017	Erwin	1
07	Use case 5 (o.b.v. patroon criteria) zakelijk portaal, eHerkenning en benodigde gegevens om (fijnmazig) te kunnen autoriseren	Afgehandeld	30 nov. 2017	Frits	1
08	Use case 6 (o.b.v. patroon criteria) toegang tot administratieve en logistieke gegevens (H2M2M)	Afgehandeld	2 nov. 2017	Brian en Erwin	2
09	Voor use case 2 toelichten welke gegevens gebruikt worden voor matching indien er geen BSN beschikbaar is.	Open	25 jan. 2018	Tine	1
10	Binnen use cases inventariseren welke koppelpunten er onderkend worden	Open	25 jan. 2018	Allen	1
11	Begrippen identiteiten / pseudoniemen definiëren/toelichten	Open	25 jan. 2018	Erwin	1
12	Uitzoeken welke attributen voor Entree Federatie resp. SURFconext nodig zijn	Open	25 jan 2018	Erwin en Sir	1
13	Uitzoeken hoe een specifiek pseudoniem wordt afgeleid bij SURFconext resp. Entree Federatie. Van het subject in de verklaring van de	Open	25 jan 2018	Erwin en Sir	1

	authenticatiedienst van de onderwijsinstelling?				

BES = Bureau Edustandaard

Grijs = afgehandeld of vervallen