Conceptversie verslag werkgroep IAA

Aanwezig:	Tom van Veen (Surfmarket), , Freek Nabuurs (Cito), Frits Bouma (DUO), Jacob Hop (Aventus, MBO), , Peter Clijsters (Surfmarket), Brian Dommisse (Kennisnet, PO/VO raad), Bram Gaakeer (OCW, voorzitter), Erwin Reinhoud (Kennisnet, Bureau Edustandaard)
Afwezig:	Tine de Mik (Studielink), Dirk Linden (Kennisnet), Edwin Verwoerd (KBb-E), Rimmer Hylkema (Thiememeulenhoff, GEU)
Agendalid:	Pieter Ruempol (GEU)

Datum en locatie
9 mei 2019, 15:00-17:00 uur, SURF , Utrecht

Agenda

1. **Opening en mededelingen**
2. **Usecases (identifiers en betrouwbaarheidsniveaus)**
3. **Voortgang en voorlopige bevindingen**
4. **Concept architectuurmodel**
5. **Rondvraag en sluiting**

1. Opening en mededelingen

Het verslag wordt zonder wijzigingen vastgesteld.

2. Usecases

2.1. ECK keten (Usecase 5 - ECKiD)

De procesanalyse van diensten binnen de ECK keten geeft een algemeen beeld. Een bepaalde dienst binnen de ECK keten kan op punten afwijken van de resultaten van de procesanalyse.

Dienst
De ECK keten usecase heeft betrekking op onderwijsvolgers die het authenticatiemiddel van de onderwijsinstelling gebruiken om toegang te krijgen tot de verschillende diensten binnen de ECK keten. De authenticatiedienst van de onderwijsinstelling is via een routeringsdienst gekoppeld aan de diensten van distributeurs en uitgevers. Voor identificatie en authenticatie wordt binnen de keten een ECKiD (sector specifieke identifier) gebruikt. Zowel distributeurs als uitgevers krijgen dezelfde identifier voor een bepaalde onderwijsvolger en gebruiken deze ook om onderling voor een bepaald persoon licentiegegevens uit te wisselen (leveren).

Betrouwbaarheidsniveau
Op basis van de regelhulp is een betrouwbaarheidsniveaus van Laag vastgesteld. Hierbij zijn de onderstaande keuzes gemaakt (zie ook team drive met rapport van regelhulp).

1. Persoonsgegevens
    a. Aard van persoonsgegevens
        i. Maximaal klasse 1 (basisniveau - beperkte set persoonsgegevens i.v.m. klantrelatie).
        ii. Er zitten kleine verschillen in de persoonsgegevens (attributenbeleid[1]) die per sector verwerkt worden.
        iii. Bij onderwijsvolgers jonger dan 16 jaar is toestemming vereist van de persoon die de ouderlijke verantwoordelijkheid voor het kind draagt. Dit wordt via school geregeld. Onderwijsvolgers ouder dan 16 handelen onder eigen verantwoording, maar leeftijd is vanuit dienstaanbieder vaak onbekend dus valt ook vaak onder verantwoordelijkheid van school.
    b. Burgerservicenummer
        i. Het BSN wordt niet verwerkt
    c. Verwerking persoonsgegevens
        i. De aard van de verwerking leidt niet tot extra risico's. Wel was in eerste instantie het ECKiD in verschillende sectoren hetzelfde voor een bepaalde onderwijsvolger. De scope is nu beperkt en de onderwijsvolger krijgt in een andere sector een andere ECKiD.
2. Er is geen rechtsgevolg[2]

[1] https://www.eck-id.nl/implementatie/documentatie

[2] Het gebruik van uw dienst kan rechtsgevolgen hebben.
Hier is sprake van als uw dienst zijn grondslag vindt in wetgeving en leidt tot rechtshandelingen. Denk bijvoorbeeld aan een besluit dat vatbaar is voor bezwaar en beroep. Maar bij uw dienst kan ook slechts sprake zijn van feitelijk handelen. Denk aan het verstrekken van inlichtingen. In dat geval is uw dienst niet op rechtsgevolg gericht. Er is nog een derde soort dienst. Die is gericht op feitelijk handelen, zoals het registreren van afvalcontainers op naam en adres. Maar dit kan vervolgens tot rechtsgevolg leiden: de gegevens gebruikt u mogelijk voor handhaving. In dat geval spreken we over indirect rechtsgevolg.

3. Er worden geen basisregistratiegegevens gewijzigd
4. Economisch belang is laag
5. Publiek belang is laag

We stellen vast dat conform de Handreiking van FS betrouwbaarheidsniveau laag vereist wordt. Het is niet duidelijk of het door de onderwijsinstelling uitgegeven middel voldoet aan de criteria die aan betrouwbaarheidsniveau laag gesteld worden. Het is wenselijk dit te onderzoeken. Ook vanuit het HO wordt aangegeven dat verfijning van eIDAS betrouwbaarheidsniveaus voor het onderwijs noodzakelijk is. Hiermee kunnen diensten binnen het onderwijs expliciet aangeven welk minimaal betrouwbaarheidsniveau vereist is en kan vanuit het (onderwijs) IAA stelsel aangegeven wat het betrouwbaarheidsniveau van de authenticatie van de onderwijsvolger is. Dit zijn in principe de activiteiten die binnen het werkpakket van IBP vallen (2.2.1 Normenkader betrouwbaarheidsniveaus voor onderwijsvolgers en medewerkers).

We merken op dat in het speciaal onderwijs het type leermiddel en de kenmerken van de onderwijsvolger voor risico verhogende factoren kan zorgen voor diensten die deze gegevens verwerken. Docentenmateriaal (toetsvragen en -antwoorden) vallen binnen de ECK keten. Het is wenselijk dat toegang tot docentenmateriaal voldoende beveiligd is. Het is niet duidelijk of het authenticatiemiddel van de onderwijsinstelling voor toegang tot docentenmateriaal wordt gebruikt. Net als bij speciaal onderwijs is het wenselijk om hiervoor een aparte analyse uit te voeren om het betrouwbaarheidsniveau vast te stellen. Er wordt hiervoor een actiepunt opgenomen (#15).

Het koppelvlak voor toegang is nu nog vaak SAML2. Er wordt opgemerkt dat dit ook in het HO het geval is. Open ID Connect (OIDC) wordt wel ondersteund, maar nog niet vaak gebruikt. De verwachting is dat dit de komende jaren wel gaat toenemen.

Identificatie

Identificatie (en autorisatie) is op basis van een sector specifieke keten identifier (ECKiD). Het ECKiD van een onderwijsvolger is specifiek voor de sector waarvoor de onderwijsvolger wordt bekostigd. Wanneer een leerling de overstap maakt van vmbo naar mbo, krijgt deze een nieuw ECKiD. Door deze beperkte scope kunnen er bij doorlopende leerlijnen gegevens van de ene sector niet aan de gegevens van de andere sector gekoppeld worden. Dit speelt bijvoorbeeld bij VMBO-MBO, VSO-VAVO, VSO-MBO en Praktijkscholen-MBO onderwijsinstelling. We constateren dat er voor doorlopende leerlijnen en sectorovergangen nog geen eenduidige oplossing lijkt te zijn. Er zijn wel een aantal workarounds bekend. Zo wordt een onderwijsvolger als onbekostigd in het VMBO ingeschreven en als bekostigd in het MBO. Door de scope te koppelen aan de bekostiging kan op deze manier dezelfde ECKiD in beide sectoren gebruikt worden. Deze workaround is in principe niet conform de privacy bevorderende maatregel om in een volgende sector een nieuwe ECKiD te gebruiken.

Binnen het onderwijs is al eerder besproken dat het wenselijk is om het individu regie op zijn/haar gegevens te geven. Een student (>16 jaar) zou dan zelf kunnen bepalen welke gegevens er bij een bepaalde partij gekoppeld worden (o.b.v. consent). Het wel of niet koppelen heeft mogelijk wel consequenties voor het onderwijsproces en deze zouden transparant moeten zijn voor een dergelijke keuze toegepast kan worden.

Het probleem rond doorlopende leerlijnen lijkt nu nog beperkt omdat in het VO en MBO nu nog vaak gescheiden leermiddelen gebruikt worden. We zien dit echter wel in de toekomst toenemen en het is wenselijk dat het mechanisme voor toegang het toepassen van doorlopende leerlijnen niet mag belemmeren. Het er op dat ECKiD op dit punt tekort schiet. Doorlopende leerlijnen zorgen niet alleen voor problemen rond het koppelen van gegevens (o.b.v. identifiers). Leerlingen die VMBO volgen, volgen in het kader van doorlopende leerlijnen ook al vaak een of meerdere dagen les bij het MBO. Dit levert problemen op bij het verschaffen van toegang tot de infrastructuur van de MBO-instelling en tot toegang van leeromgevingen en –middelen die de leerling wil/moet gebruiken (usecase 6B).

Vanuit Edu-K is eerder een ander vraagstuk rond het ECKiD en leerhistorie vastgesteld. Als een leerling, bijvoorbeeld door een verhuizing, de overstap maakt van de ene po-school naar de andere po-school, blijft het ECKiD gelijk, maar verandert het bevoegd gezag. Dit betekent dat de koppeling tussen het ECKiD en de opgebouwde leerhistorie ongedaan gemaakt wordt. Binnen de werkgroep hebben we niet kunnen vaststellen of dit een obstakel is of dat het juist wenselijk is dat bij de nieuwe po-school de ‘oude’ leerhistorie niet beschikbaar is. Er wordt een actiepunt opgenomen om navraag hierover te doen (#16)

Rond het SAML koppelvlak constateren we dat het format van de technische sleutel (SAML Subject NameID) waarschijnlijk gehandhaafd blijft en dat het ECKiD als attribuut geleverd wordt. Standaard software voor SAML ziet in principe de NameID als de identiteit binnen de authenticatieverklaring. Partijen moeten de software aanpassen om de ECKiD te gebruiken voor de keyring koppeling aan de interne identifier voor de onderwijsvolger.

HO (usecases rond het eduID)

Binnen het HO spelen een aantal vraagstukken rond toegang, zoals bijvoorbeeld het studentmobiliteit. De volgende usecase worden toegelicht:

1. Usecase 1A: Toegang student (HO) bij andere instelling – Aanmelding en inzage in opleidingsgegevens

2. Usecase 1C: Toegang student bij andere instelling – Toegang ELO.
3. Usecase 1F: Toegang burger – Bring Your Own ID

EduID is nog in ontwikkeling en de architectuur en belangrijke implementatie details worden nu uitgewerkt en het plan is om dit in 2019 af te ronden. De usecases geven een beeld in welke situaties eduID bij toegang een rol kan gaan spelen. Hiermee worden de eerste kaders beschreven waar het eduID aan moet voldoen. Hiermee wordt echter nu nog niet duidelijk hoe toegang concreet geregeld gaat worden met eduID. We willen met de procesanalyse nu een beeld kunnen vormen over hoe toegang (identifiers en betrouwbaarheidsniveaus) in verschillende sectoren is geregeld.

Er wordt aangegeven dat EduID gebruik wil gaan maken van pseudoniemen als identifiers voor dienstverleners en instellingen. Deze partijen krijgen dan elk een andere identifier terwijl zij soms wel gegevens moeten delen. In die situatie speelt eduID ook een rol als “resolver” van deze identifiers, waarbij de student de interactie tussen die partijen toestaat.

Er wordt afgesproken om de volgende keer een aantal kenmerken van eduID nader te bespreken zodat we iets meer zicht hebben of en hoeverre dit aansluit bij andere toekomstbeelden.

3. Afsluiting

Status werkpakketten
De werkgroep is nog bezig met de procesanalyse. Op basis van de bevindingen die bij de bespreking van de usecases naar voren zijn gekomen willen de komende periode per doelgroep generieke patronen voor toegang definiëren.

Werkpakket	Adviesorgaan	Status	Opmerkingen
2.1.1 Normenkader betrouwbaarheidsniveaus voor burgers en bedrijven (Wet Digitale Overheid)	OCW/WDO	In uitvoering	Het programma eID (onderdeel WDO) heeft als opdracht het opleveren van authenticatiediensten op betrouwbaarheidsniveau Substantieel en Hoog. Het programma ontzorgt (overheids-)dienstverleners door aansluiting op deze authenticatiediensten te vergemakkelijken. Als de behandeling van de wet volgens planning verloopt treed de wet rond 1 juli 2019 in werking. De voorlopig gehanteerde criteria voor betrouwbaarheidsniveaus komen uit de Handreiking van het Forum Standaardisatie. De criteria uit de Handreiking betrouwbaarheidsniveaus dienen als vertrekpunt maar er wordt nog wel gewerkt aan de criteria die uiteindelijk worden opgenomen in uitvoeringsregelgeving onder de Wet digitale overheid (WDO).
2.1.2 Aansluitschema onderwijs (WDO)	OCW/WDO	In uitvoering	We hebben hiermee een overzicht van diensten binnen het onderwijsdomein die (verplicht) op het eID stelsel moeten aansluiten. De procesanalyse (usecase) maakt vervolgens duidelijk welke (architectuur) kaders hierbij gelden en hoe identificatie is geregeld (identifiers) bij overgangen en ketenprocessen. We zijn al een aantal diensten tegengekomen bij de procesanalyse.
2.2.1 Normenkader betrouwbaarheidsniveaus voor onderwijsvolgers en medewerkers	IBP Werkgroep	Uitgesteld (in afwachting van meer concretere kaders en rationale vanuit IAA werkgroep)	Er is nog geen normenkader betrouwbaarheidsniveaus voor onderwijsvolgers en medewerkers beschikbaar. De IBP werkgroep heeft dit nog niet kunnen behandelen. De IAA werkgroep is ondertussen wel met de procesanalyse gestart. Belangrijke inpunt hiervoor zijn de betrouwbaarheidsniveaus en de criteria die hiervoor gelden. Voorlopig wordt hiervoor de handreiking van Forum Standaardisatie gebruikt. Dit geeft mogelijk tevens inzicht of het vereist is dat er een apart normenkader betrouwbaarheidsniveaus voor onderwijsvolgers en medewerkers komt. De IAA werkgroep zal de ervaringen met de IBP werkgroep delen. Vanuit SURF is aangegeven dat eIDAS betrouwbaarheidsniveaus als uitgangspunt genomen kan worden, maar zal, wil het relevantie hebben voor het HO, meer fijnmazig moeten worden uitgewerkt door bijvoorbeeld de niveaus laag en substantieel nader te detailleren. Hierdoor wordt mogelijk ook een handreiking met criteria voor deze niveaus relevant. De werkgroep IBP komt niet vaak bij elkaar. Voor een bijeenkomst is het wenselijk om de rationale voor extra niveaus (en een handreiking) scherp te hebben. De IAA werkgroep zit momenteel nog in de fase om dit vast te stellen. Als we aanvullende niveaus willen onderkennen wat is dan de (juridische) betekenis hiervan?
2.3 Procesanalyse	Regiegroep	In uitvoering	De diensten van DUO (2.3.1) en Studielink (2.3.2) en MBO Centraal Aanmelden (2.3.5) zijn geanalyseerd. We hebben meer inzicht gekregen in de betrouwbaarheidsniveaus en identifiers die via het eID stelsel geleverd worden. Diensten in ECK keten (2.3.4) en Hoger Onderwijs (2.4.1) moeten nog geanalyseerd worden. Vooralsnog zullen de diensten van Basispoort (2.3.3) niet geanalyseerd worden.

Volgende overleg
De volgende bijeenkomst is op 18 juni 2019 van 14:30 tot 17:00 uur.

4. Actielijst

#	Omschrijving	Status	Einddatum	Actie-houder
01	Aanleveren hoe governance geregeld is (proces rond afstemming met achterban)	Afgerond	Voor 23 oktober	IAA WG
02	Nieuwe versie projectplan opleveren	Afgerond	Oktober 24	BES
03	Review commentaar	Afgerond	Voor 31 oktober	IAA WG
04	Voorzitter KBb-E vragen om vertegenwoordiging in regiegroep	Afgerond	Oktober	BES
05	IBP werkgroep gaat betrouwbaarheidsniveaus normenkader agenderen voor IBP WG	Open	Juni 2019	IBP WG
06	Bij de procesanalyses wordt de toepasbaarheid van de handreiking en de eIDAS betrouwbaarheidsniveaus getoetst	Open	Juni 2019	IAA WG
07	In checklist het veld 'Toekomstbeeld of huidige situatie' opnemen.	Afgerond	April 2019	BES
08	Het gebruik van de handreiking bij analyse van diplomaregister	Afgerond	April 2019	DUO
09	Analyse usecase 2 (doelgroep internationale student) en toegang tot studielink voor medewerkers van onderwijsinstellingen	Afgerond	April 2019	Studielink
10	Analyse usecase 5	Afgerond	April 2019	BES/Thiememeulenhoff
11	Navraag bij Basispoort over bijdrage usecase 9	Afgerond	April 2019	BES
12	Opstellen van checklist usecase 4	Afgerond	April 2019	BES/SaMBO-ICT
13	Opstellen van checklist usecase 1	Afgerond	April 2019	SURF
14	Platform om documenten te delen	Afgerond	April 2019	BES
15	Analyse diensten rond speciaal onderwijs en docentenmateriaal	Open		BES/ IAA WG
16	Navraag bij Edu-K over ontkoppeling tussen het ECKiD en de opgebouwde leerhistorie bij overstap naar andere po-school.	Open		BES

BES = Bureau Edustandaard
Grijs = afgehandeld of vervallen