Conceptversie verslag werkgroep IAA

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

Datum en locatie
25 januari 2018, 13:00-15:00 uur, SURF-net , Utrecht

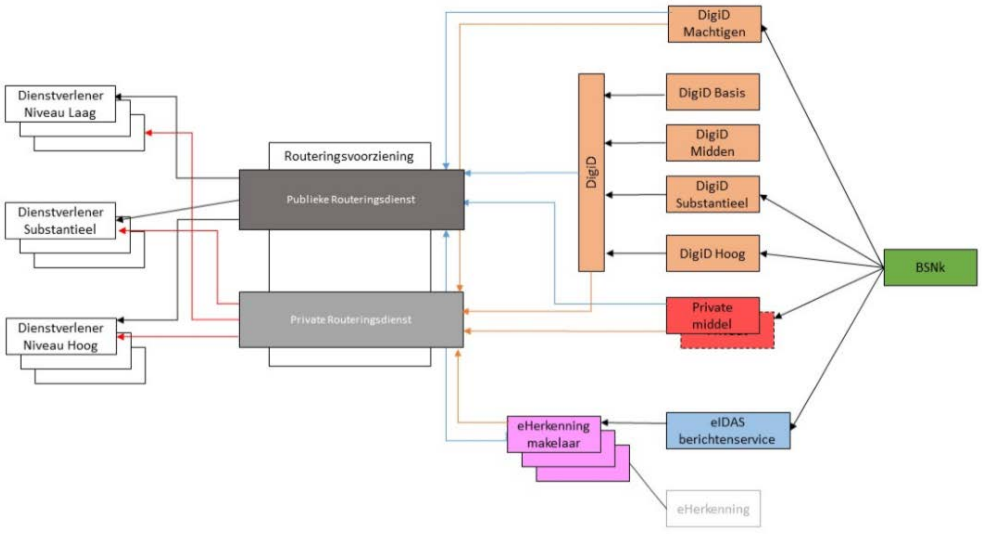
Agenda

1. **Opening, mededelingen, vaststellen agenda**
2. **Vaststellen verslag van 30 november 2017 en actielijst**
3. **Toelichting en bespreking notitie**
4. **Start feitelijke analyse initiatieven**
5. **Vervolg afspraken inplannen**
6. **Rondvraag**
7. **Afsluiting**

1. Opening, mededelingen, vaststellen agenda

Bram merkt op dat de use case van het lerarenregister wordt meegenomen in de analyse, maar er zullen geen deelnemers vanuit het lerarenregister project aanschuiven.

De naam van de Wet generieke digitale infrastructuur (GDI) is verandert in Wet digitale overheid (DO). De Wet digitale overheid is reeds naar de Raad van State gestuurd. Tijdens een bijeenkomst bij OCW werd de Wet digitale overheid aan belanghebbenden toegelicht. Het blijft nog onduidelijk wanneer deze wet precies ingaat. Daarnaast zal er een overgangstermijn gelden om partijen de ruimte te geven om de nodige wijzigingen door te voeren. De nadruk ligt nu bij het eID stelsel voor burgers, hoe e.e.a. voor bedrijven/medewerkers precies vorm gegeven gaat worden is nog onduidelijk, maar we gaan er nog steeds vanuit dat eHerkenning hier een belangrijke rol in zal spelen. Om dienstaanbieders die toegang verlenen aan burgers te ontlasten is er een nieuw concept geïntroduceerd, de routeringsvoorziening. Omdat er ook een privaat middel voor burgers gaat komen en een eIDAS koppelvlak beschikbaar moet zijn voor EU burgers, worden de dienstaanbieders met de routeringsvoorziening ontlast doordat zij slechts één koppelvlak hoeven te implementeren en waarschijnlijk ook met één partij financiële zaken kunnen afhandelen (zie figuur).



Bij de ICTU is er een werkgroep authenticatie gestart om in de NORA[1] meer zaken op het gebied van IAA op te nemen. Als het materiaal tijdig beschikbaar komt dan zullen we deze overnemen indien dit van onze begrippen/concepten afwijkt. De zaken die uiteindelijk in de ROSA opgenomen gaan worden zullen aansluiten op de NORA begrippen en concepten.

De agenda wordt zonder wijzigingen vastgesteld.

2. Doornemen verslag en actielijst van 30 november 2017

Tine geeft aan een aantal opmerkingen op het verslag te hebben, deze zullen nog door haar worden nagestuurd. Het verslag zal hierop worden aangepast. Er zijn geen andere opmerkingen op het verslag.

Tine geeft terugkoppeling op actiepunt #9: welke gegevens gebruikt worden voor matching indien er geen BSN beschikbaar is. Er is geen BSN als er is ingelogd met een Studielink-account. De persoonsgegevens die in deze situatie naar de onderwijsinstelling gestuurd worden zijn o.a. NAW gegevens, geboortedatum en geslacht. De onderwijsinstelling controleert deze tegen de identiteitsdocumenten van de student. Uiteindelijk controleert DUO deze gegevens in het BRP. Indien dit geen resultaat oplevert en er dus geen BSN is, wordt gecontroleerd of er wel een onderwijsnummer voor deze persoonsgegevens bestaat. Als dit niet het geval is dan creëert DUO een nieuw onderwijsnummer. DUO communiceert het PGN (onderwijsnummer of BSN) terug naar SL en onderwijsinstelling[2].

Het komt voor dat een student zich direct bij de onderwijsinstelling zelf inschrijft. In het geval dat het een bekostigde student betreft dan worden de gegevens van de student alsnog naar SL gestuurd. Er wordt opgemerkt dat we nog geen eenduidige definitie van een bekostigde student hebben. Tine stelt voor deze aan te leveren (actiepunt #14).

Actiepunt 11, nieuw begrip *Identifier*. Vorige keer werd opgemerkt dat we vaak de term *identiteit* gebruiken, maar dat het dan vaak niet een zuivere identiteit betreft. Het studielinknummer of een specifiek pseudoniem zijn namelijk geen identiteiten. Om in algemene zin naar dit soort begrippen te kunnen verwijzen is het begrip identifier toegevoegd. De definitie hiervan luidt :"*Een label (meestal een string of tekst) waarmee je een entiteit aanduidt*. Toelichting: Dit maakt het mogelijk om naar een entiteit te verwijzen. Zo'n entiteit heeft meestal meerdere identifiers die in verschillende contexten nuttig kunnen zijn. Een dienstaanbieder kan met een identifier naar een bepaald persoon verwijzen. De identifier van een bepaalde dienstafnemer wordt door het IAA-stelsel geleverd. Voorbeelden hiervan zijn het BSN of een specifiek pseudoniem.".

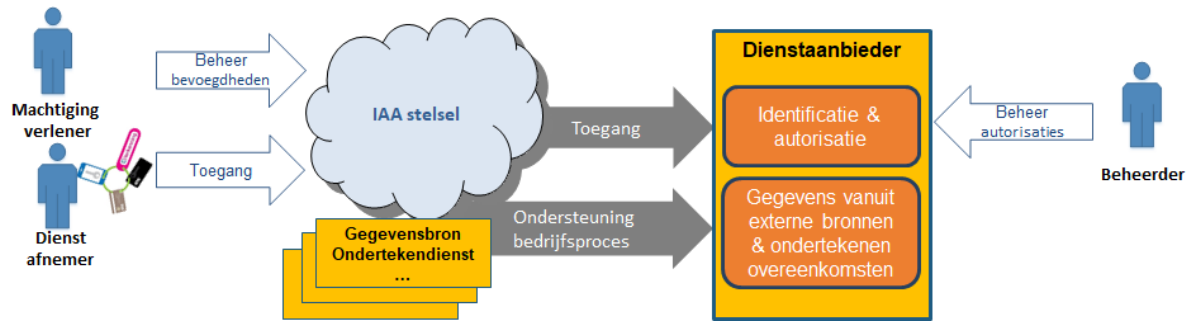
3. Toelichting en bespreking notitie

We onderkennen in de notitie een vijftal belangrijke aandachtsgebieden, dit zijn:

1. Identifiers, het bereik, de betrouwbaarheidsniveaus en koppelpunten
2. Attributen t.b.v. toegang
3. Autorisatie en machtigingen
4. Attributen levering t.b.v. ondersteuning van het bedrijfsproces
5. Koppelvlakken, protocollen en transformaties

Het figuur hieronder geeft een hoog over beeld van alle relevante aandachtsgebieden.

[1] https://www.noraonline.nl/wiki/NORA_online
[2] Dit is nu zeer generiek gedefinieerd en zou indien nodig sectorspecifiek beschreven kunnen worden.



De verschillende aandachtsgebieden die in de notitie staan beschreven worden toegelicht.

Identifiers, bereik, de betrouwbaarheidsniveaus en koppelpunten
De identifier die een dienstaanbieder ontvangt is vaak verschillend afhankelijk van het gekozen toegangskanaal (stelsel/toegangsdienst/authenticatiedienst). In een overzicht is aangegeven welke verschillende identifiers er zoals vanuit verschillende stelsels geleverd worden.

Om tot een eenduidige vergelijking van identifiers te komen is er gekeken naar de verschillende koppelvlakken van de stelsels (vulling NameID in het SAML-koppelvlak). In de vergelijking komt duidelijk naar voren dat Entree Federatie en SURFconext hier heel verschillend mee omgaan. Ook het eHerkenning stelsel geeft zijn eigen invulling hieraan en gaat mogelijk op termijn ook migreren naar identifiers op basis van polymorfe pseudoniemen. In de tabel hieronder worden de identifiers van Entree Federatie, SURFconext en eHerkenning (beperkt aantal uit de 1.11e versie) weergegeven.

Naam	SURFconext	Entree Federatie	eHerkenning (1.11e)
Identifier (SAML NameID) urn:oasis:names:tc:SAML:2.0:nameid-format:persistent urn:oasis:names:tc:SAML:2.0:nameid-format:transient NB: onduidelijk of AD in het MBO de NameID hetzelfde vult voor SURFconext als Entree Federatie. SURFconext vult overigens de NameID met eigen nieuwe persistente UUID.	The user's identity is transmitted in the form of the NameID element. Every IdP must supply a NameID, but for privacy reasons SURFconext will generate a new one, which is duplicated in the attribute eduPersonTargetedID (urn:mace:dir:attribute-def:eduPersonTargetedID). Format:urn:oid:1.3.6.1.4.1.5923.1.1.1.10 (string: bd09168cf0c2e675b2def0ade6f50b7d4bb4aae) To identify a user the Service Provider must use NameID or eduPersonTargetedID. NameID is guaranteed to be stable for a fixed user (except in the case of transient identifiers). SURFconext will generate a NameID for each new user. It is unique for the user and specific to the SP	**uid** Uniek ID van de gebruiker. Dit is een versleutelde versie van de gebruikersnaam en het employeeNumber, gevolgd door de omgeving (realm) Format: hash@realm Voor een SAML koppeling moet de waarde van het uid attribuut gelijk zijn aan de waarde van het <saml:NameID> veld Het eckId attribuut wordt gebruikt als persistente identifier voor een dienstafnemer in de eck keten in een bepaalde onderwijssector	BSN (9 cijfers) Consumer - Een specifiek pseudoniem dat wordt gebruikt om een consument te identificeren binnen Idensys (32 byte hex ABCDEF1234567890ABCDEF1234567890ABCDEF1234567890ABCDEF1234567890). Pseudo - Een specifiek pseudoniem (SP) dat wordt gebruikt om een consument te identificeren binnen eHerkenning (32 byte hex). In the event of representation, this value is followed by an @ and hexadecimal value of 16 byte.

Bij de bespreking van de koppelpunten ontstaat er wat discussie. Het overzicht klopt niet en wordt als te abstract beschouwd. Ook ontstaat er discussie of DUO in deze use case als koppelpunt gezien kan worden, is er daadwerkelijk een transformatie, een overgang van de ene identifier naar de andere? Een verdere analyse moet uitwijzen of hier sprake van is en of dit relevant is voor ons (actiepunt #15). Het belang hiervan hangt ook samen met de vraag of het werken met een onderwijsnummer dat onafhankelijk is van het BSN (qua vorm en qua afleiding) als belangrijk onderwerp wordt gezien.

Attributen t.b.v. toegang

Het gaat hier om attributen die typisch door de toegangsdienst geleverd worden. Attributen die geleverd worden bij gebruik/ondersteuning bedrijfsproces worden mogelijk geleverd via een ander kanaal dat beter is ingericht om een dienst fijnmazig aanvullende persoonsgegevens (op basis van doelbinding) of andere gegevens te leveren

Attributen t.b.v. toegang worden geleverd om efficiënt de autorisatie te ondersteunen. De gegevens die bij toegang geleverd worden ondersteunen het autorisatieproces bij de dienstaanbieder. Een dienstafnemer kan bijvoorbeeld geautoriseerd worden op basis van enkel de identifier, of het attribuut *rol*, of op basis van een *entitlement* attribuut.

Toegangsdiensten Entree Federatie en SURFconext gebruiken soms dezelfde en soms verschillende attributen voor hetzelfde gegeven. Voor de organisatie wordt een ander attribuut gebruikt en ook de vulling is anders. Als het attribuut hetzelfde is, is niet duidelijk of het gegeven van dezelfde bron afkomstig is. Komt bijvoorbeeld de *eduPersonAffiliation* die SURFconext van de authenticatiedienst geleverd krijgt vanuit dezelfde bron als die Entree Federatie van de authenticatiedienst in het MBO geleverd krijgt? De onderstaande tabel geeft een aantal voorbeelden.

Naam	**SURFconext**			**Entree Federatie**			**Opmerking**
	Attribuut	**Omschrijving**	**Voorbeeld**	**Attribuut**	**Omschrijving**	**Voorbeeld**	
Login naam	urn:mace:dir:attribute-def:uid	The uid is not a unique identifier for SURFconext users. Uid values are at most unique for each IdP	s9603145 piet flåp@example.edu	- (zie uid)			Dit login attribuut bestaat bij Entree Federatie wel (uid) maar wordt bij Entree Federatie als de Identifier gebruikt (SAML NameID)
Organisatie	urn:mace:terena.org:attribute-def:schacHome Organization (urn:oid:1.3.6.1.4.1.25178.1.2.9)	Organisation's domain name	uniharderwijk.nl	nlEduPersonHomeOrganizationId (standaard attribuut*) nlEduPersonHomeOrganization (standaard attribuut*)	BRIN van de instelling Naam van de instelling	1ZZ03 Petteflat College	Organisatie wordt verschillend geïdentificeerd
Rol	urn:mace:dir:attribute-def:eduPersonAffiliation (urn:oid:1.3.6.1.4.1.5923.1.1.1.1)	Indicates the relationship between the user and his home organisation (multi-valued)	employee, student, faculty, member, affiliate, pre-student	eduPerson Affiliation (standaard attribuut*)	Rol	student, employee, staff of affiliate	Geen gestandaardiseerde rollen. Onduidelijkheid bij mulitvalue, is dit comma seperated string?
Entitlement	urn:mace:dir:attribute-def:eduPersonEntitlement	Custom URI that indicates an entitlement. This attribute can be used to communicate entitlements from identity providers to	urn:mace:terena.org:tcs:personal-admin				Entitlement kan helpen bij authorisatie vraagstukken.

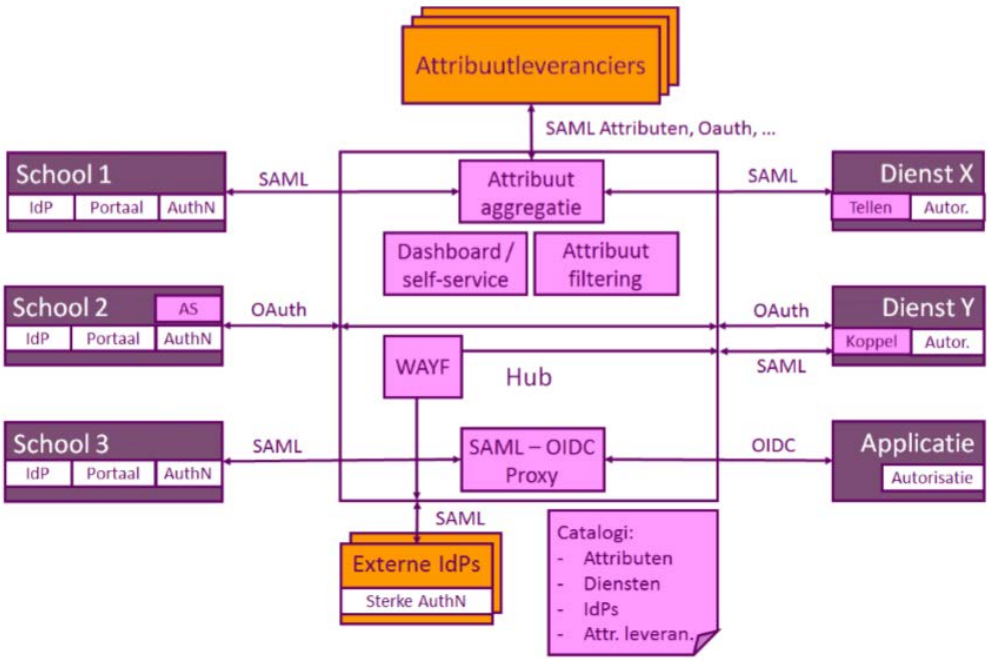
		services for authorization					
Kopie van NameID als attribuut	urn:mace:dir:attribute-def:eduPersonTargetedID urn:oid:1.3.6.1.4.1.5923.1.1.1.10	The attribute eduPersonTargetedID is a copy of the Subject -> NameID which is generated by SURFconext itself.	bd09168cf0c2e675b2def0ade6f50b7d4bb4aae				ID wordt ook als attribuut doorgegeven.

Ook de overige onderwerpen worden nog kort toegelicht.

Er wordt opgemerkt dat in de notitie ook ouders genoemd worden en dat de identificatie van ouders van een ander niveau is dan bijvoorbeeld de processen bij DigiD. In tekst moet duidelijk aangegeven worden dat het identificeren van ouders niet van een bepaald betrouwbaarheidsniveau is. Op basis van eIDAS betrouwbaarheidsniveaus zou over het algemeen wel gesteld kunnen worden dat dit op betrouwbaarheidsniveau Laag wordt gedaan.

4. Start feitelijke analyse initiatieven

De volgende keer zal de analyse van de initiatieven centraal staan en de leden wordt gevraagd deze nog eens door te nemen. Het document *Toekomstperspectief toegang* bevat het onderstaande figuur welke wel overeenkomsten heeft met ons beeld van een toegangsdienst. We willen vaststellen of we in de initiatieven herkenbare knelpunten en oplossingen terugzien, of dat deze nieuwe onderkennen, of wellicht zaken ontbreken, of in tegenspraak zijn met elkaar of met onze bevindingen. De brondocumenten (initiatieven) worden met de uitnodiging voor het volgende overleg meegestuurd.



5. Afsluiting

Het volgende overleg is op 1 maart van 13:00 tot 15:00 uur.

6. 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.	Afgehandeld	25 jan. 2018	Tine	1
10	Binnen use cases inventariseren welke koppelpunten er onderkend worden	Afgehandeld	25 jan. 2018	Allen	1
11	Begrippen identiteiten / pseudoniemen definiëren/toelichten	Afgehandeld	25 jan. 2018	Erwin	1
12	Uitzoeken welke attributen voor Entree Federatie resp. SURFconext nodig zijn	Afgehandeld	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	Afgehandeld	25 jan 2018	Erwin en Sir	1

	verklaring van de authenticatiedienst van de onderwijsinstelling?				
14	Definitie bekostigde student/instelling	Afgehandeld, opgenomen bij begrippen.	Feb 2018	Tine	2
15	Identifier koppelpunten tussen onderwijsinstellingen, DUO en Studielink inzichtelijk maken indien vastgesteld is dat dit relevant voor het onderzoek is.	Open	Feb 2018	BES	1

BES = Bureau Edustandaard

Grijs = afgehandeld of vervallen