Toekomstbeeld Toegang (IAA)

Van:	Edustandaard werkgroep IAA
Aan:	Architectuurraad
Versie:	0.7
Status:	Concept
Datum:	Oktober 2020

Inhoudsopgave

1. Inleiding

1.1. Achtergrond

De werkgroep Toegang is geïnitieerd door de Standaardisatieraad[1]. Opdracht van de werkgroep Toegang is om in kaart te brengen op welke wijze de toekomstbeelden voor toegang binnen de onderwijssectoren op elkaar aansluiten, vast te stellen welke issues problemen geven met de aansluiting en een aanpak voor te stellen waarmee de aansluiting geborgd kan worden. Als eindresultaat heeft de werkgroep een aanpak beschreven voor de ontwikkeling van een sectoroverschrijdend toekomstbeeld toegang, die wordt beschreven in dit document.

1.2. Doel

Het doel is om bij toegang de persoon centraal te stellen. Een persoon kan ook handelen namens een Niet Natuurlijk Persoon (rechtspersoon). Een persoon kan meerdere rollen hebben: lerende, onderwijsprofessional of onderzoeker, of medewerker (handelend namens rechtspersoon). Bij elke rol kan de persoon verschillende rechten hebben. Bij toegang moet gezorgd worden dat de toegang makkelijk wordt gemaakt voor de persoon in kwestie en dat tegelijkertijd regie op gegevens mogelijk is: de persoon krijgt toegang tot de gegevens waar deze vanuit zijn rol recht op heeft, niet meer maar ook niet minder. Bij regie op gegevens wordt voldaan aan de vigerende wetgeving zoals AVG, WDO, EIDAS en de onderwijswetgeving.

Toegang voor lerende
Toegang wordt ingericht vanuit het perspectief van de lerende zodat een leven lang leren wordt ondersteund.

Toegang voor onderwijsprofessional
Toegang wordt ingericht vanuit het perspectief van de onderwijsprofessional zodat deze op een consistente wijze toegang krijgt tot leeromgeving en administratieve systemen, onafhankelijk van de onderwijsaanbieder en de leverancier.

Toegang voor onderzoeker
Toegang wordt ingericht vanuit het perspectief van de onderzoeker zodat deze op een consistente wijze toegang krijgt tot onderzoeksdata, onafhankelijk van de bron.

Toegang voor medewerker
Toegang wordt ingericht vanuit het perspectief van de rechtspersoon zodat de medewerker op een consistente wijze toegang krijgt tot de dienst en kan handelen namens rechtspersoon.

[1] https://www.edustandaard.nl/oprichting-werkgroep-iaa-inventarisatie/

1.3. Probleemstelling

In de huidige situatie verschilt de wijze van toegang tussen:

- Sectoren
- Toepassingsgebieden, bijvoorbeeld contentketen, administratieve processen en onderzoek.
- Erkend en niet erkend onderwijs
- Initieel en post-initieel onderwijs.

De consequentie is dat bij instellings- en sectoroverschrijdende use cases het lastig is om bij toegang de balans te vinden tussen gebruiksvriendelijkheid enerzijds en borgen van privacy en beveiliging anderzijds. Daarnaast zijn de gekozen oplossingen onvoldoende flexibel waardoor aanpassingen lastig, tijdrovend en kostbaar zijn. Terwijl anderzijds de behoefte aan flexibiliteit steeds groter wordt door steeds strengere eisen aan privacy en beveiliging. Er ingespeeld moet worden op overheidsbrede en Europese bewegingen zoals eHerkenning, EIDAS, etc. En er een toenemende behoefte komt aan flexibiliteit in het onderwijs en het ondersteunen van doorlopende leerlijnen. Deze doorlopende leerlijnen vergen ook betere aansluiting tussen initieel en post-initieel onderwijs. En betere aansluiting tussen erkend onderwijs, private opleidingen en beroepsonderwijs.

1.4. Werkwijze

De werkwijze is er op gericht om er voor te zorgen dat architectuur helpt bij het tegengaan van verschotting. Dit begint met inzicht gegeven in de huidige situatie. Er wordt aangegeven in welke situaties er problemen zijn met de aansluiting en wat hiervan de consequenties zijn. De vervolgstap is om voorstellen te doen voor betere aansluiting. De verbetervoorstellen kunnen verwerkt worden in een doelarchitectuur die een beeld geeft van toegang in de gewenste situatie.

Dit stelt eisen aan de architectuur. De architecturen van sectoren en toepassingsgebieden moeten op elkaar aansluiten. Een gemeenschappelijke referentie architectuur kan helpen deze aansluiting mogelijk te maken. In dit document wordt een referentiearchitectuur toegang beschreven die ingepast moet kunnen worden in de ROSA. Deze referentiearchitectuur bevat kaders die het mogelijk maken toegang vanuit perspectief van de persoon in te richten en regie op gegevens mogelijk te maken. Deze kaders zijn opgesteld op basis van issues die de aansluiting belemmeren. De issues zijn vastgesteld aan de hand van een inventarisatie van usecases (zie overzicht op ROSA wiki[2]) die gericht zijn op sectorovergangen en onderzoek naar relevante ontwikkelingen op gebied van wetgeving, standaarden en infrastructuur.

[2] https://www.wikixl.nl/wiki/rosa/index.php/Werkgroep_IAA

1.5. Doelgroep

De doelgroep van dit document is de Architectuurraad ROSA. Het is de bedoeling de aspectarchitecuur toegang wordt opgenomen in de ROSA. Op basis van dit document zullen beslispunten opgesteld worden voor de Standaardisatieraad. Besluitvorming door de Standaardisatieraad gebeurt op basis een beslisnota met dit document als bijlage.

1.6. Leeswijzer

De referentiearchitectuur toegang wordt beschreven in de hoofdstukken 2 tot en met 7. Voor de de structurering wordt het ROSA architectuur raamwerk gebruikt waarbinnen de architectuurkaders voor toegang zijn ingevuld. De ROSA sluit aan bij de NORA. Het thema toegang (IAA) is bij de NORA nog in ontwikkeling. De NORA definieert een begrippenkader dat wordt overgenomen in dit document. De NORA onderkent een (Dienst)Afnemer die een Dienst afneemt en verschillende functies die het toegangsproces ondersteunen (identiteitenbeheer, authenticatiemiddelenbeheer en bevoegdheden beheer). Hiervoor worden requirements beschreven. De NORA requirements worden meegenomen en waar nodig aangevuld en toegespitst op de onderwijscontext.

Architectuurkaders zijn bedoeld voor het realiseren van doelstellingen en het oplossen van knelpunten. Door de koppeling met usecases wordt duidelijk gemaakt welke knelpunten in de huidige situatie opgelost moeten worden. De gebruikte usecases zijn beschreven in bijgevoegde bijlage. Op basis van een analyse is vastgestelde welke toegang issues in de huidige situatie gesignaleerd zijn bij sector overgangen. Deze issues zijn opgenomen in hoofdstuk 8. Een issue komt vaak voor in meerdere usecases, dit onderstreept dat er een gedeeld belang is om het issue op te lossen. Hoofdstuk 8 vormt de verbinding met de bijlage. Hoofdstuk 9 geeft aan op welke wijze de issues worden opgelost, met 2 opties:

- Optie 1: opstellen architectuurkaders.
  De werkgroep lost het issue op met een architectuurkader.
- Optie 2: definiëren actiepunten
  De werkgroep definieert een actie die wordt gerelateerd aan de corresponderende issues. Hoofdstuk 9 biedt een overzicht met alle uit te voeren acties, geclusterd per verantwoordelijke actor en met statusinformatie over de afhandeling van de openstaande acties.

Wanneer alle issues zijn opgelost bevatten hoofdstuk 2 tot/en met 9 de doelarchitectuur toegang. De doelarchitectuur toegang zal worden opgenomen in de ROSA zodat de samenhang met andere thema's bewaakt kan worden. Er zijn procesafspraken nodig om de actiepunten uit hoofdstuk 9 te beleggen. Hiervoor is besluitvorming in de Standaardisatieraad nodig.

Toegang is een van de thema's die uitgewerkt worden binnen de ROSA. Voor elk van deze thema's worden architectuurkaders opgesteld. Deze architectuurkaders moeten op elkaar aansluiten, de ROSA moet zorgen voor samenhang. Hierdoor ontstaan afhankelijkheden. Architectuurkaders die voor een ander thema worden uitgewerkt kunnen randvoorwaardelijk zijn voor toegang. Deze afhankelijkheden moeten expliciet gemaakt worden om de samenhang binnen de ROSA te kunnen bewaken.

2. Structurering architectuurkaders

De ROSA streeft een modulaire architectuur na met zo veel mogelijk cohesie binnen modules en beperkte afhankelijkheden tussen modules. Hierdoor kunnen architectuurkaders binnen een module worden aangepast zonder dat dit effect heeft voor de rest van de architectuur. Dit vergroot de flexibiliteit en maakt hergebruik mogelijk. Bij een modulaire architectuur worden afhankelijkheden in kaart gebracht, tussen modules onderling en tussen doelstellingen en modules. Binnen de ROSA vindt de afbakening van modules plaats op basis van 2 criteria: architectuurlagen en functionaliteiten. Bij architectuurlagen wordt onderscheid gemaakt tussen organisatie-, informatie- en applicatie laag. De beleidsdoelstellingen en de wettelijke kaders zijn richtinggevend voor de organisatielaag. De informatie- en applicatielaag zijn ondersteunend voor de organisatielaag. Bij de functionaliteiten wordt onderscheid gemaakt tussen de ondersteunende en de administratieve processen.

3. Scope toegang

3.1. Wat verstaan we onder toegang (IAA)

In dit document wordt een aanpak beschreven voor de ontwikkeling van een sectoroverschrijdend toekomstbeeld toegang. Hierbij verstaan we onder toegang de functies waar een dienstaanbieder gebruik van maakt om een autorisatiebeslissing te kunnen nemen. De functies die hierbij een rol spelen zijn Identificatie, Authenticatie en Autorisatie.

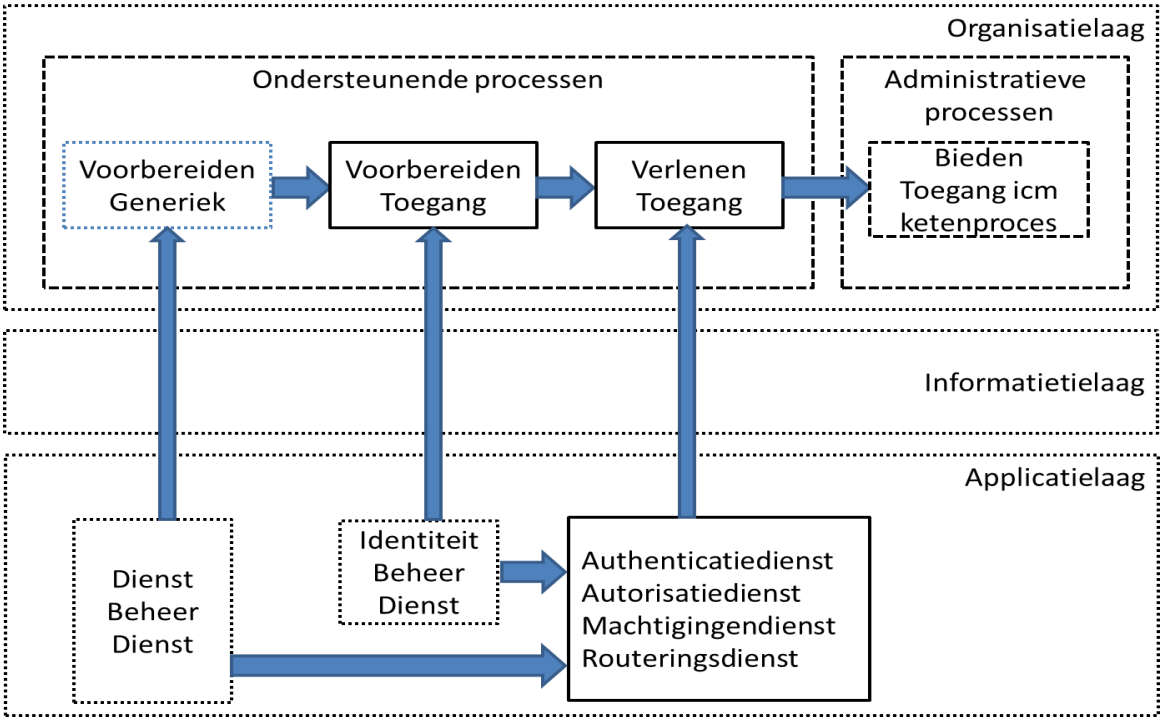
3.2. Uitbreiding ten opzichte van NORA scope

De NORA scope van toegang is beperkt tot verlenen toegang (identiteitenbeheer, authenticatiemiddelenbeheer en bevoegdheden beheer). De ROSA scope omvat hiernaast de relaties met architectuurkaders van andere thema's:

- Randvoorwaardelijk voor ondersteunen toegang zijn gedefinieerde diensten en een vastgesteld betrouwbaarheidsniveau. Voorbereiding generiek is een ondersteunend proces dat zorgt voor het invullen van deze randvoorwaarden.
- Er zijn architectuurkaders nodig om eisen te stellen aan de wijze van interactie die nodig is voor toegang. De architectuurkaders toegang omvatten patronen die aangeven welke interactie plaatsvindt.

Onderstaand plaatje geeft de scope weer van ROSA architectuurkaders voor toegang:

- Bij de ondersteunende processen zijn de processen "voorbereiden generiek" en "bieden toegang" een uitbreiding op de NORA scope.
- Binnen de applicatielaag zijn "dienst beheerdienst" en "identiteit beheerdienst" een uitbreiding op de NORA scope



Figuur 1- Scope van ROSA architectuurkaders voor toegang

3.3. Toelichting ROSA scope

3.3.1. Organisatielaag

Ondersteunende processen

- Voorbereiden generiek
  Dit proces zorgt voor bepalen betrouwbaarheidsniveau en definiëring van diensten. Dit proces is randvoorwaardelijk voor "voorbereiden toegang"
- Voorbereiden toegang.
  Dit proces zorgt voor "identiteitenbeheer", "beheer van authenticatiemiddelen" en "bevoegdhedenbeheer". Dit proces is randvoorwaardelijk voor "ondersteunen toegang".
- Verlenen toegang
  De toegangscontrole wordt uitgevoerd door "verlenen toegang", een real-time proces dat zorgt voor "authenticatie", "autorisatie" en "machtigen". Dit proces is randvoorwaardelijk voor "Toegang icm ketenproces(sen)".
- *Toegang icm ketenproces(sen)*
  Het afnemen van een dienst kan aanleiding zijn voor een bepaald ketenproces (M2M gegevensuitwisseling). Deze kan niet zomaar plaatsvinden. Hiervoor moeten procesafspraken worden gemaakt waarbij mogelijk de interactie tussen dienstafnemer en dienstaanbieder een rol speelt, maar ook tussen gegevensafnemer en gegevensverstrekker. De dienstaanbieder kan de rol van gegevensafnemer of gegevensverstrekker hebben. De dienstafnemer kan betrokkene zijn.

3.3.2. Informatielaag

In de informatielaag worden de begrippen gedefinieerd die nodig zijn voor toegang. Dit omvat definiëring van diensten, taken, bevoegdheden en identificerende kenmerken. Hierbij wordt ook de relatie gelegd kunnen met wettelijke kaders.

3.3.3. Applicatielaag

“dienst beheerdienst” levert applicatiediensten die randvoorwaardelijk zijn voor het proces “voorbereiden generiek” en de applicatiediensten “autorisatiedienst” en de “machtigingendienst”

"Identiteit beheerdienst" levert applicatiediensten die randvoorwaardelijk zijn voor het proces “voorbereiden toegang” en de applicatiedienst “authenticatiedienst”.

“authenticatiedienst”, “autorisatiedienst”, “machtigingendienst” en “routeringsdienst” leveren applicatiediensten die randvoorwaardelijk zijn voor het proces “verlenen toegang”.

4. Architectuurkaders organisatielaag

4.1. Rollen

Samenwerking vereist afspraken over de rollen en de eisen die gesteld worden aan rollen.
De rol van dienstafnemer moet gedefinieerd zijn en het moet duidelijk zijn welke eisen gesteld worden aan deze rol. De ROSA sluit hier aan bij de wetgeving. De ROSA begrippenlijst[3] definieert een aantal begrippen die relevant zijn voor het thema IAA. In dit document wordt beschreven welke eisen hieraan gesteld worden in de context van IAA.

4.1.1. Dienstafnemer

Karakteristieken dienstafnemer
Een dienstafnemer is een natuurlijk persoon die gebruik maakt van de dienst. De dienstafnemer doet dit namens zichzelf of namens een andere partij (natuurlijk persoon of rechtspersoon. Voordat er toegang verleend wordt moet de dienstafnemer voldoen aan de eisen die de dienstaanbieder voor de dienst stelt.

- Het kan zijn dat de dienstafnemer zich moet authenticeren. Hiervoor wordt dan het authenticatiemiddel gebruikt dat voldoet aan deze eisen.
- Aan het verkrijgen en gebruik van het authenticatiemiddel zijn voorwaarden verbonden die samenhangen met het vereiste betrouwbaarheidsniveau.
- Een dienstafnemer is een natuurlijk persoon die een dienst afneemt. Binnen de rol dienstafnemer kunnen verschillende doelgroepen onderscheiden worden, zoals bijvoorbeeld Nederlandse burger of student. Welke doelgroep het betreft kan worden bepaald door de context van de dienst of het authenticatiemiddel dat de dienstafnemer gebruikt. Met het onderkennen van doelgroepen kan er een generiek beeld gevormd worden hoe toegang geregeld is.
- Een natuurlijk persoon kan de dienst namens zichzelf afnemen of namens een andere partij (natuurlijk persoon of niet natuurlijk/rechtspersoon). Een voorbeeld van een doelgroep waarbij een dienstafnemer namens een niet natuurlijk persoon een dienst afneemt is de medewerker.
- Het authenticatiemiddel waarover een bepaalde doelgroep beschikt (bijvoorbeeld een leerling die over het authenticatiemiddel beschikt dat de school heeft uitgegeven) kan voor meerdere diensten gebruikt worden (bijvoorbeeld de digitale leermiddelen die door verschillende partijen voor de school beschikbaar zijn gesteld).
- Voor een dienstafnemer en het gebruikte authenticatiemiddel kan het relevant zijn of de dienst van een organisatie is die verantwoordelijk is voor het uitvoeren van wettelijke taken en diensten van private partijen.

Wetgeving begrippen
In de wetgeving kunnen eisen worden gesteld die gekoppeld zijn aan de rol. Op basis hiervan moet onderscheid worden gemaakt tussen wetgeving rollen:

- Europese burger
  Een dienstaanbieder die binnen de scope van de EIDAS verordening valt moet het voor Europese burgers mogelijk maken dat zij kunnen inloggen met hun nationaal (genotificeerd) authenticatiemiddel kunnen inloggen. De Europese burger wordt geïdentificeerd met het Uniqueness ID[4]. De Europese burger kan op enig moment meerdere uniqueness ID's hebben.
- Nederlandse burger. In de WDO is vastgelegd op welke wijze een Nederlandse burger toegang krijgt tot overheidsdiensten die geleverd worden door dienstverleners die gerechtigd zijn het BSN te gebruiken.

[3] https://www.wikixl.nl/wiki/rosa/index.php/Begrippenlijst_ROSA
[4] Een Europese burger kan op enig moment meerdere uniqueness ID's hebben

- Niet Europese burger, natuurlijke personen die als niet Europese burger een dienst afnemen. Voor het te gebruiken authenticatiemiddel is geen wettelijk kader anders dan eventuele wetten die hier indirect betrekking op hebben, bijvoorbeeld de AVG, BIR en BIO.
- Onderwijsvolger. Een onderwijsvolger is een Mens die een opleiding volgt, heeft gevolgd of gaat volgen of opgaat of is opgegaan voor een toets. Onderwijsvolgers binnen het bekostigd onderwijs worden over het algemeen geïdentificeerd met het Persoonsgebonden Nummer (PGN). Bij onderwijsvolgers wordt onderscheid gemaakt tussen personen die jonger zijn dan 16 jaar en personen die ouder zijn dan 16 jaar. Bij onderwijsvolgers die jonger zijn dan 16 jaar zijn moet rekening worden gehouden met kaders ten aanzien van wettelijke vertegenwoordiging.
- Medewerker
  Een medewerker is een natuurlijk persoon die werkt voor een niet natuurlijk persoon (instelling of leverancier). Het bevoegd gezag van de niet natuurlijke persoon heeft de medewerker gemachtigd om de dienst af te nemen..
- Onderwijsprofessional
  Een onderwijsprofessional is een medewerker van een instelling die bevoegd is om onderwijs te geven.

4.2. Architectuurkaders processen

4.2.1. Voorbereiding generiek

Voorbereiding generiek heeft als doel te zorgen voor:

1. Transparante kaders
   Dienstafnemer kan verifiëren welke kaders gelden voor afname van deze dienst.
2. Transparantie bij verwerking
   Dienstafnemer kan verifiëren welke afspraken zijn gemaakt met verwerkers.
3. Transparantie over transacties met gegevens
   Dienstafnemer kan verifiëren welke transacties zijn gedaan met zijn persoonsgegevens.
4. Kwaliteitsbeheersing processen
   Dienstafnemer kan verifiëren welke maatregelen zijn genomen om de kwaliteit te borgen
5. Doelmatigheid

Transparante kaders

Overheidsorganisaties voeren wettelijke taken uit. In de wet is vastgesteld welke persoonsgegevens gebruikt mogen worden en welke randvoorwaarden gelden voor toegang.

1. Te specificeren wat de dienst inhoudt (NORA AP5)
   Een dienstverlener zorgt voor een dienstbeschrijving die vindbaar is
2. Te specificeren hoe de dienst is ontsloten (NORA AP9)
   Opnemen in de dienstbeschrijving via welke URL de dienst kan worden aangeroepen
3. Te specificeren welk type identifier de dienst vereist (transient, targeted of shared).
   Voor het gebruikte authenticatiemiddel en/of doelgroep wordt aangegeven welke identifier gebruikt wordt.
4. Vaststellen betrouwbaarheidsniveau.
   De dienstverlener bepaalt het minimale betrouwbaarheidsniveau van de authenticatieverklaring. Op basis van een risicoanalyse en een vastgestelde handreiking (bijvoorbeeld de handreiking van Forum Standaardisatie[5] en de regelhulp tool).
5. Het maken van afspraken met dienstafnemer over de levering van de dienst (NORA AP28)
   a. De dienstafnemer (beoogde doelgroep) beschikt over passende authenticatiemiddelen.
   b. Afspraken over de verwerking van (persoons)gegevens voor de dienst kunnen zowel in de voorbereidings- als de uitvoeringsfase worden gemaakt.

[5] Forum standaardisatie (WDO)

Transparantie bij verwerking
Een dienstaanbieder kan gebruik maken van een verwerker die bij gerelateerde ketenprocessen namens de dienstaanbieder met een M2M koppeling gegevens uitwisselt met andere partijen. De verwerker is een niet natuurlijk persoon die in opdracht van de dienstaanbieder een bijdrage levert aan het leveren van de dienst. Hiervoor moeten formele afspraken worden gemaakt over rechten en plichten. Dit mandaat wordt vastgelegd in een serviceregister (van de dienstaanbieder) zodat partijen die via de M2M koppeling gegevens ontvanger kunnen verifiëren dat de verwerker namens de dienstaanbieder optreedt (gemandateerd is).

Transparantie over transacties met gegevens
De diensten worden geleverd ter ondersteuning van bepaalde processen. Een proces voert transacties uit waarbij gegevens worden geraadpleegd en/of gemuteerd. Een betrokkene kan opvragen welke activiteiten uitgevoerd worden om de dienst te leveren, welke transacties op zijn gegevens zijn uitgevoerd en welke actor de transactie heeft uitgevoerd.

Kwaliteitsbeheersing processen
Aan de processen worden kwaliteitseisen gesteld. Een van deze kwaliteitseisen is een genormeerd betrouwbaarheidsniveau van de authenticatie. De authenticatie zelf is slechts voor een deel bepalend voor het betrouwbaarheidsniveau. De processen rond identiteitsverificatie en registratie (persoons)gegevens en het uitgifteproces van het authenticatiemiddel hebben hier ook invloed op.

Doelmatigheid
Om de afhankelijkheid van externe identifiers te voorkomen zullen dienstaanbieders de externe identifier die vanuit het IAA stelsel geleverd wordt koppelen aan een interne identifier. Bij het gebruik van verschillende toegangskanalen (IAA stelsels) kan deze interne identifier gebruikt worden om de verschillende externe identifiers te koppelen.

4.2.2. Voorbereiding toegang

Om toegangscontrole mogelijk te maken moeten "identiteitenbeheer", "beheer van authenticatiemiddelen" en "bevoegdhedenbeheer" zijn ingericht.

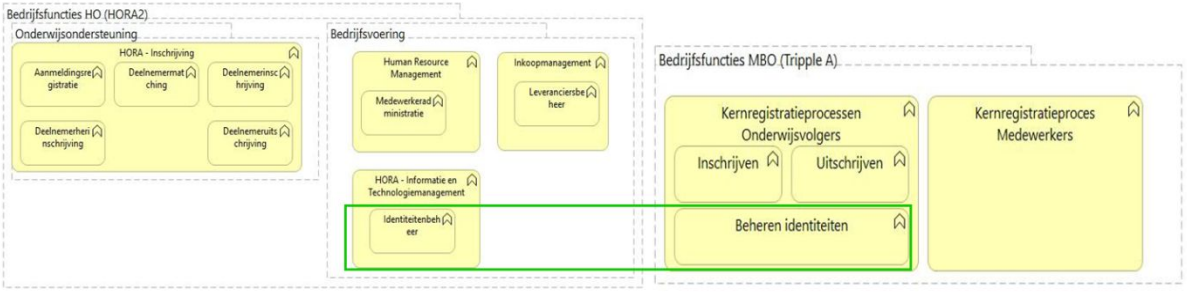
Identiteitenbeheer (Identity Management)
Identiteitenbeheer begint met de creatie van een digitale identiteit door bepaalde kenmerken te registreren. Het zijn digitale afspiegelingen van zogenaamde entiteiten (personen, bedrijven, computers, apps of IoT e.d.). Deze digitale identiteit maakt identificatie in de digitale wereld mogelijk. Deze identiteiten worden waar nodig gewijzigd en uiteindelijk beëindigd.

- Het identiteitenbeheer is mede bepalend voor het betrouwbaarheidsniveau bij authenticatie.
- Het betrouwbaarheidsniveau wordt bepaald met een gestandaardiseerd normenkader, bijvoorbeeld dat van eIDAS[6] dat eisen stelt aan het identiteitenbeheer van Europese burgers. Het normenkader van de eIDAS bepaalt de gestelde eisen aan het identiteitenbeheer[7].
- Het identiteitenbeheer stelt eisen aan de informatielaag. Het gaat om gegevens zoals de naam, geboortedatum, BSN, fysiek adres, rijbewijsnummer en paspoortnummer. In specifieke gevallen ook gegevens als bijvoorbeeld sector- of ketenidentifier, functie, groep, opleiding.
- Het identiteitenbeheer voor Nederlandse burgers wordt via de BRP[8] geregeld.
- Onderwijsinstellingen zijn beheerders van digitale identiteiten van onderwijsvolgers en onderwijsprofessionals (zie Triple A en HORA Figuur 2). Voor erkend onderwijs geldt dat DUO de identiteiten van de onderwijsvolgers verifieert.
- DUO beheert de (identificerende) gegevens van onderwijsinstellingen. Momenteel wordt hiervoor vaak het BRIN4 voor gebruikt, maar in de MBO en VO sector wordt al gebruik

[6] https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32014R0910&qid=1510307152543
[7] https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32015R1502
[8] https://wetten.overheid.nl/BWBR0033715/2019-02-03

gemaakt van het RIO en de digitale identiteiten (van onderwijsaanbieders) die hierin beheerd worden.

- Het identiteitenbeheer maakt gebruik van de applicatielaag, de gegevens worden beheerd in een identiteitenbeheervoorziening. De school gebruikt als identiteitenbeheervoorziening voor onderwijsvolgers een LAS/SIS en een HR systeem voor onderwijsprofessionals. De identiteiten van onderwijsinstellingen worden geregistreerd in RIO .



Figuur 2 - Identiteitenbeheer is onderdeel van Triple A en HORA

Authenticatie(middelen)beheer

Dit betreft de "levenscyclus" van authenticatiemiddelen in relatie tot digitale identiteiten.
Hiertoe regel je enerzijds het ontwikkelen, aanpassen en verwijderen van authenticatiemiddelen in de vorm van "verificatiediensten", die met een bepaalde zekerheid aangeven in welke mate een digitale identiteit overeenkomt met de entiteit (natuurlijk persoon) waaraan die is toegekend. En anderzijds regel je het toekennen van authenticatiemiddelen aan digitale identiteiten of het intrekken daarvan.
Het betrouwbaarheidsniveau van een uitgevoerde authenticatie wordt dus bepaald door enerzijds de kwaliteit van de identiteiten(registratie) en anderzijds het daarbij gebruikte authenticatiemiddel.

- Het authenticatiemiddelenbeheer is mede bepalend voor het betrouwbaarheidsniveau van de digitale identiteit. Een organisatie die het authenticatiemiddelenbeheer uitvoert moet zich houden aan de eisen van het betrouwbaarheidsniveau normenkader dat ondersteund wordt.
- De Wet Digitale Overheid (WDO) stelt regels op voor een authenticatiemiddel voor Nederlandse burgers en bedrijven die aansluiten bij de Europese regels (eIDAS).
- Tot het authenticatiemiddelenbeheeer beheer behoort ook de uitgifte van fysieke authenticatiemiddelen (hardware tokens). Deze worden na uitgifte door de dienstafnemer beheert (gebruiksfase van de levenscyclus). Het fysieke beheer valt buiten scope van de informatiearchitectuur
- Het authenticatiemiddelenbeheer stelt eisen aan de informatielaag. Het gaat om gegevens zoals Identifiers, account en eventuele aanvullende attributen. Of om informatie over fysieke authenticatiemiddelen (telefoon, USB sleutel, softtoken).
- Het authenticatiemiddelenbeheer maakt gebruik van applicatiedienst voor beheren gegevens.

Bevoegdhedenbeheer

Het Bevoegdhedenbeheer[9] wordt ook wel Autorisatiebeheer of Access Management genoemd. Om toegang te verlenen ben je er nog niet als je weet welk digitale identiteit toegang vraagt: je moet weten of de digitale identiteit de juiste rechten heeft om toegang te verkrijgen. Uitgangspunt hierbij is, dat met bepaalde "regels" wordt bepaald wat mag (of wat niet mag) en dat op het moment dat ergens toegang tot wordt gevraagd, dat dan wordt gecontroleerd of dat volgens die regels mag. De bevoegdheden kunnen grof en fijnmazig zijn en tevens generiek, dan wel specifiek per dienst. Bevoegdheden zijn hierdoor niet statisch en zullen dus wijzigen in de loop van de tijd.

De NORA definieert het machtigen als onderdeel van bevoegdheden beheer. In bredere context kan dit zo gezien worden. We willen hier echter benadrukken dat het bevoegdhedenbeheer als een verantwoordelijkheid van de dienstaanbieder wordt gezien. Het beheer van een machtiging kan worden gezien als een verantwoordelijkheid van een dienstafnemer.

[9] https://www.noraonline.nl/wiki/Bevoegdhedenbeheer

- Het bevoegdhedenbeheer is een functie van de Dienstaanbieder.
- Machtigen wordt gezien als een onderdeel van Bevoegdhedenbeheer. Het machtigingenbeheer is echter een functie van de Dienstafnemer.
- Het bevoegdhedenbeheer heeft een relatie met identiteitenbeheer en authenticatiemiddelenbeheer.
- Gegevens binnen het identiteitenbeheer kunnen bepalend zijn voor de bevoegdheden van een dienstafnemer.
- Via provisioning kan ervoor gezorgd worden dat gegevens aan de gewenste systemen (diensten) geleverd kunnen worden.

4.2.3. Verlenen toegang

Het doel van verlenen toegang is te verifiëren of de dienstafnemer een dienst mag afnemen. Verlenen toegang is een real-time proces. De uniforme voorbereidende processen die hier aan vooraf gingen zorgen ervoor dat toegang conform afspraken gerealiseerd wordt. Het proces is grotendeels geautomatiseerd. De procesrol omvat de bewaking van de geautomatiseerde activiteiten en het herstel van eventuele fouten.

Karakteristieken ondersteunen toegang

- Verlenen toegang is een functie van de Dienstaanbieder
- Verlenen toegang maakt een vergelijking tussen de bevoegdheden die worden gevraagd voor het afnemen van een dienst en de bevoegdheden waarover de aanvrager beschikt. Deze autorisatie vindt plaats op basis van de door het IAA stelsel geleverde gegevens (digitale identiteit).
- De digitale identiteit betreft verschillende gegevens en zijn afhankelijk van de context. De context wordt bepaald door enerzijds de dienstafnemer en anderzijds door de dienst.
- De digitale identiteit kan een identifier zijn, maar ook andere gegevens of een combinatie. Bij het gebruik van het authenticatiemiddel worden deze in een Authenticatieverklaring door de Authenticatiedienst aan de dienstaanbieder geleverd. Het is wenselijk dat de verklaring die de identifier bevat ook het betrouwbaarheidsniveau van de authenticatie aangeeft.
- Verlenen toegang maakt gebruik van de volgende applicatiediensten:
    - Authenticatiedienst, deze heeft interface om de dienstafnemer zich te kunnen laten authenticeren en een interface om de dienstaanbieder de Authenticatieverklaring (van een bepaald betrouwbaarheidsniveau) te leveren.
    - Authenticatie Hub (optioneel).
      Dienst die verzoeken voor gebruikersauthenticatie van dienstverleners routeert naar de authenticatiediensten van die gebruikers (dwz doorgeefluik van authenticatieverzoeken). Attributendienst voor leveren aanvullende gegevens. Deze aanvullende gegevens zijn niet nodig voor authenticatie maar voor het uitvoeringsproces. De Attributendienst heeft een interface voor gegevensuitwisseling met ketenpartners.

4.2.4. Toegang icm ketenproces

Bij het leveren van een dienst aan een dienstafnemer (H2M) kan er ook sprake zijn van een gerelateerd ketenproces waarbij gegevens uitgewisseld worden tussen de dienstaanbieder en een ketenpartner. Bij samenwerking in de keten moeten afspraken gemaakt over de wijze van interactie om deze gecombineerde H2M en M2M gegevensuitwisseling te realiseren. Hiervoor worden interactiepatronen gedefinieerd. Voor elk patroon wordt gedefinieerd:

- Welke rollen worden onderscheiden
- Afspraken over wijze van interactie tussen de rollen bij verlenen van toegang en uitwisseling van gegevens
- Gebruik dat wordt gemaakt van ondersteunende processen en applicatiediensten

De volgende interactiepatronen worden onderkend:

Initiëren dienst
Initiëren dienst beschrijft de interactie die plaatsvindt tussen dienstaanbieder en dienstafnemer om tot een overeenkomst te komen met de voorwaarden voor het leveren van de dienst.
Bij initiëren van de dienst vindt toegangscontrole plaats om te verifiëren dat de initiator gerechtigd is de aanvraag te doen. Dit geldt dus ook voor de eventueel aan de dienst gerelateerde gegevensuitwisseling. De initiator kan de betrokkene zijn of diens gemachtigde.

Leveren diensten
Leveren dienst beschrijft de interactie die plaatsvindt tussen dienstverlener en betrokkene bij het leveren van de dienst.

Initiëren gegevenslevering
Initiëren gegevenslevering beschrijft de interactie die plaatsvindt tussen dienstaanbieder (als gegevensleverancier of gegevensafnemer) en ketenpartner om tot een overeenkomst te komen voor uitwisseling van gegevens die onderdeel vormen van het ketenproces en de dienst.

Verstrekken gegevens
Verstrekken gegevens beschrijft de interactie die plaatsvindt tussen gegevensleverancier en gegevensafnemer bij het uitwisselen van gegevens.

Verstrekken van procesinformatie
Wettelijk is vastgelegd onder welke condities een actor kan opvragen welke gegevensleveringen zijn uitgevoerd. Wanneer een dergelijke actor deze informatie opvraagt moet deze verstrekt worden.

Kenmerken interactiepatronen:
- De processen moeten de beschreven interactiepatronen ondersteunen.
- Het interactiepatroon beschrijft op welke wijze gebruik wordt gemaakt van het ondersteunende proces “verlenen toegang”.
- Bij het aanvragen van dienst of gegevenslevering moet een dienstafnemer zijn digitale identiteit en bevoegdheden verstrekken. Op basis hiervan kan bij verlenen toegang de bevoegdheidsbepaling en autorisatie plaatsvinden.
- Diensten worden geleverd aan een aanvrager met de vereiste bevoegdheden.
- Bij ketenprocessen wordt gebruik gemaakt van de volgende applicatiediensten:
    - Ondersteunen administratief proces
    - Verstrekken procesinformatie

5. Architectuurkaders informatielaag

5.1. Normenkaders betrouwbaarheidsniveau

Er zijn verschillende normenkaders voor het definiëren van het betrouwbaarheidsniveau. Bij de voorbereiding van de dienstverlening moeten de relevante processen (identiteitenbeheer, authenticatiemiddelenbeheer) aan de eisen van dit normenkader voldoen.

- Het normenkader van eIDAS[10] wordt binnen WDO toegepast en kent drie niveaus: Laag, Substantieel en Hoog.
- Het EN-ISO/IEC 29115 normenkader is de basis voor de betrouwbaarheidsniveaus van SURFsecureID[11] en NEN7510/NEN7512[12]. Dit normenkader kent 4 niveaus: Laag, Midden, Hoog en Zeer Hoog. SURFsecureID wordt toegepast binnen de SURF doelgroep (MBO, HBO, WO, UMC's, Research), NEN7510/NEN7512 geldt binnen de zorg.

5.2. Type identifiers

5.2.1. Persistentie en scope

Identifiers kunnen ingedeeld worden op basis van hun persistentie en de scope waarin een bepaalde identifier gebruikt wordt. Op basis hiervan worden de volgende typen identifiers onderkend:

1. Shared
2. Targeted
3. Transient

Shared Identifier
Dit type identifier is persistent (wordt gebruikt in meerdere sessies) en wordt door meerdere diensten (dienstaanbieders) gebruikt. Het gebruik hoeft het niet alleen toegang te betreffen, het kan ook gebruikt worden bij een (gerelateerde) M2M gegevensuitwisseling waarbij verschillende ketenpartijen dezelfde identifier gebruiken om naar een persoon te kunnen verwijzen (communicatie over persoon). Voor het gebruik van de shared identifier bestaan randvoorwaarden, de dienstaanbieder moet door het IAA stelsel identificeerbaar zijn en tot de betreffende scope van de shared identifier behoren. Bij toegang moet dit vastgesteld kunnen worden om bij elke sessie de identifier te kunnen leveren.

Targeted Identifier
Dit type identifier is persistent en is dienst specifiek, een bepaalde dienst (dienstaanbieder) krijgt dezelfde unieke identifier (bij elke sessie). Voor het kunnen leveren van de targeted identifier bestaan randvoorwaarden, het IAA stelsel moet de dienstaanbieder kunnen identificeren om bij elke sessie dezelfde identifier te kunnen leveren.

Transient Identifier
Dit type identifier is niet persistent, voor elke sessie wordt er een andere identifier geleverd. Voor kunnen leveren van de transient identifier bestaan randvoorwaarden, bij toegang mag er niet dezelfde identifier geleverd worden (bijvoorbeeld door te werken met een GUID).

[10] https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32015R1502

[11] https://wiki.surfnet.nl/display/SsID/Using+Levels+of+Assurance+to+express+strength+of+authentication

[12] https://www.webtoolmanagementsystemen.nl/nl/NormDetail?standardId=cc28b925-3d18-4036-bd60-196465c9a05b

5.2.2. Overzicht identifiers

Naam	Domein	Type	Toegang	Keten	Opm.
AanmeldingID	Onderwijs	Shared		CA	
BSN	Overheid	Shared	eID	Zie PGN	In nabije toekomst in eID versleutelt als polymorfe identiteit
ECKiD	Onderwijs	Shared	EF/SC/BP	ECK	
eduPersonPrincipalName	Onderwijs	Shared	SURFconext (SC)		
ESI	Onderwijs	Shared	HO	Erasmus	
Leerling id	Onderwijs	Shared	Basispoort (BP)		
nlEduPersonProfileId	Onderwijs	Shared	Entree Federatie (EF)		
nlEduPersonRealId	Onderwijs	Shared	Entree Federatie (EF)		
nlEduPersonTargetedId	Onderwijs	Targeted	Entree Federatie (EF)		
ON	Onderwijs	Shared		Zie PGN	

ORCID	Onderwijs	Shared	SURFconext		
PGN	Onderwijs	Shared		OSO / Studielink / Centraal Aanmelden	Is BSN of Onderwijs Nummer
schacPersonalUniqueCode	Onderwijs	Shared	SURFconext		
Studielinknummer	Onderwijs	Shared		Studielink	
uid	Onderwijs	Shared	Entree Federatie (EF)		

5.2.3. Gebruikte identifiers voor natuurlijke personen binnen het onderwijs

PGN
Het persoonsgebonden nummer (PGN[13]) is de unieke identificatie van een natuurlijk persoon die in Nederland erkend onderwijs volgt. Als deze persoon een BSN heeft vormt dit het PGN. Als de persoon geen BSN heeft wordt de persoon uniek geïdentificeerd door een Onderwijsnummer (OWN) dat door DUO wordt toegekend. Op het moment dat een persoon een BSN krijgt moet het OWN ingetrokken worden en gaat dit BSN vanaf dan in het onderwijs gelden als PGN.

BSN
1. Het BSN is shared identifier
2. Het BSN is een persoonsgegeven.
3. De toepassing van het BSN is aan wetgeving gebonden.
4. Het BSN wordt gebruikt bij toegang (communicatie met persoon) om een Nederlandse burger te identificeren.
5. Het BSN wordt in het overheidsdomein bij ketenprocessen gebruikt om eenduidig naar een bepaald persoon te kunnen verwijzen (communicatie over persoon). Het voorkomt een matchingsvraag bij gegevensuitwisseling tussen ketenpartijen en dat elke partij persoonsgegevens aan de burger vraagt (eenmalige gegevensverstrekking, meervoudig gebruik). Bepaalde partijen (DUO) mogen een BSN verwerken en persoonsgegevens ophalen bij BRP. Bij ketenuitwisseling wordt soms naast het BSN ook een Ketenidentifier geleverd. Het volstaat dan om bij vervolgstappen de Ketenidentifier mee te sturen.
6. Het eID en eIDAS stelsel leveren aan bevoegde dienstaanbieders een BSN.

ECKiD

[13] https://www.rijksoverheid.nl/onderwerpen/privacy-en-persoonsgegevens/burgerservicenummer-bsn/bsn-in-het-onderwijs

Het ECKiD wordt op basis van o.a. een BSN door de Nummervoorziening gepseudonimiseerd. Er zijn voorschriften[14] om het pseudoniem bij transport en opslag te versleutelen.

1. Het ECKiD is wordt in een specifieke onderwijssector en keten toegepast (sector waarvoor de onderwijsvolger wordt bekostigd).
2. Het ECKiD wordt in de ECK keten gebruikt om eenduidig naar een bepaald persoon te kunnen verwijzen (communicatie over persoon). Het gebruik van een ECKiD voorkomt dat er een matchingsvraag ontstaat bij gegevensuitwisseling tussen ketenpartijen.
3. Het ECKiD wordt ook gebruikt bij toegang om een onderwijsvolger te identificeren (communicatie met persoon).

Studielinknummer

1. Het Studielinknummer is een shared identifier
2. Het Studielinknummer wordt in HO ketens gebruikt om eenduidig naar een bepaald persoon te kunnen verwijzen (communicatie over persoon).

AanmeldingID (Shared Identifier)

1. Het AanmeldingID is een shared identifier
2. Het AanmeldingID van VA MBO wordt in ketens gebruikt om eenduidig naar een bepaald persoon te kunnen verwijzen (communicatie over persoon).

[14] https://developers.wiki.kennisnet.nl/images/b/b9/Voorschriften_verwerken_ECK_ID.pdf

5.2.4. Gebruikte identifiers voor natuurlijke personen binnen IAA stelsels

Identifiers via SURFconext[15]
De SURFconext federatie genereert zowel targeted als transient identifiers voor dienstverleners op het moment van inloggen door studenten of medewerkers. Welke identifier doorgegeven wordt is afhankelijk van de afspraken met de betreffende dienstverlener. Deze identifier wordt in het eduPersonTargetedID veld opgenomen.

Daarnaast kunnen ook identifiers vrijgegeven worden door de aangesloten instellingen of andere autoritatieve bronnen, en via SURFconext doorgegeven worden aan een dienstverlener of andere instelling. Welke identifiers doorgegeven worden is afhankelijk van de afspraken met de betreffende dienstverlener.

- eduPersonPrincipalName; een shared identifier met de vorm "user@scope", waarbij de "user" de identifier van de persoon binnen de instelling is en "scope" meestal de instelling weergeeft.
- schacPersonalUniqueCode; een shared identifier met de gebruiker's student- of medewerkernummer uit de interne systemen van de instelling.
- ECKiD; een shared identifier uit de Educatieve Contentketen
- ORCID; is een shared identifier voor researchers die uitgedeeld wordt door ORCID.org

[15] https://wiki.surfnet.nl/display/surfconextdev/Attributes+in+SURFconext

Identifiers via Entree Federatie[16]
Met Entree Federatie hebben dienstafnemers (medewerkers en leerlingen) toegang tot digitale educatieve diensten (zoals Wikiwijs, Beeld en Geluid op school en Nieuwsbegrip) voor scholen in het po, vo en mbo. Voor het authenticeren gebruiken de dienstafnemers een schoolaccount of een Entree-account.

Entree Federatie geeft verschillende identifier(s) als attribuut door aan de dienstaanbieder. Welke dit zijn wordt deels bepaald door de afspraken (Attribute Release Policy[17]) van de onderwijsinstelling met de betreffende dienstverlener. Er zijn standaard attributen die altijd doorgegeven worden en optionele attributen de expliciet in de ARP benoemd moeten worden.

ECK Keten Identifiers (Shared)
- VO[18] ECKiD[19] (nu ook nog nlEduPersonRealId[20])
- MBO ECKiD (nu ook nog nlEduPersonProfileId[21])

Overige Identifiers
- uid[22] (Shared)
- nlEduPersonTargetedId (Targeted)

Identifiers via Basispoort
Met Basispoort hebben dienstafnemers 'Single Sign On' toegang tot online software van de aangesloten uitgeverijen en aanbieders van digitale leer- en werkomgevingen voor leerlingen, leerkrachten en ondersteunende medewerkers van basisscholen.

UWLR 2.3 (juni 2020) zorgt ervoor dat per leerling één van de volgende drie situaties ter identificatie van de leerling kunnen voorkomen:

- Alleen "ECK-iD" (bij voorkeur),
- Beide "ECK-iD" en "Leerling id" (met LAS-key),
- Alleen "Leerling id" met LAS-key (alleen als leerling geen ECK-iD heeft)

Er zijn standaard attributen die altijd worden doorgegeven en optionele attributen.

Voor docenten kunnen "ECK-ID" en "Leerkracht-ID" voor identificatie worden gebruikt. Een ECK-iD ter identificatie van de leerkracht kan vaak niet worden toegepast. Optioneel kan het emailadres worden gebruikt. Vanaf start schooljaar 2020-2021 heeft Basispoort standaard voor iedere school, per groep in het LAS van de school, een "anoniem account" voor een invalleerkracht. Op de dag van invallen kan dit invalaccount (op basis van naam en emailadres) worden geactiveerd door de ICT-coördinator.

[16] https://developers.wiki.kennisnet.nl/index.php?title=KNF:Attributen_overzicht_voor_Service_Providers
[17] https://support.kennisnet.org/Knowledgebase/Article/View/511
[18] Het is ook mogelijk om het ECK iD in het PO door te geven via Entree Federatie.
[19] Standaard attribuut mits de Service Provider zich hiervoor heeft aangemeld via: https://www.kennisnet.nl/entree-federatie/aanmelden/, uniek ECK pseudoniem voor leerling of docent
[20] Optioneel attribuut, nlEduPersonRealId is de onversleutelde versie van het uid dat als standaard attribuut geleverd wordt (userId@realm).
[21] Optioneel attribuut, indien een school meerdere administraties voert kan het administratienummer worden toegevoegd achter het @-teken
[22] Standaard attribuut, Uniek ID van de gebruiker. Dit is een versleutelde versie van de gebruikersnaam en het employeeNumber, gevolgd door het @-teken en de omgeving (hash@realm). Dezelfde waarde wordt gebruikt voor de vulling van het SAML NameID.

5.2.5. Ontwikkelingen rond identifiers voor natuurlijke personen

EduID
Het doel van eduID[23] is om de student zelf een digitale identiteit te geven voor een flexibele en levenslange onderwijs carrière. In tegenstelling tot de huidige situatie waarin de instellingen de digitale identiteit beheert, staat met eduID de student centraal. Met eduID ligt de regie bij de student zelf.

1. Het eduID is een voorziening die targeted identifiers afgeeft.
2. Een student heeft dus niet 1 eduID, maar voor iedere dienstaanbieder een andere. Hiermee kunnen dienstaanbieders of instellingen niet zomaar zien dat het over dezelfde persoon gaat.
3. Soms is dit wel nodig (bijvoorbeeld in een keten), dan kan onder regie van de student de uitgedeelde eduID's aan elkaar gelinkt worden.
4. eduID zorgt voor privacy en regie bij gegevensoverdracht tussen instellingen onderling, tussen instellingen en diensten of tussen dienstverleners onderling.

European Student Identifier (ESI)
De ESI is een shared identifier die vanaf 2021 gebruikt gaat worden binnen het Erasmus uitwisselingsprogramma. Het ESI wordt gebruikt om de student in de administratieve keten te identificeren, en om de student tijdens het inloggen te herkennen. Het ESI is ontwikkeld door het MyAcademicID project[24], wat weer onder het European Student Card initiative (ESCi) programma valt.

- Het ESI heeft de vorm:
  urn:schac:personalUniqueCode:<country-code>:<eNS>:<sHO>:<code>
  - <country-code> is een twee letter afkorting van het land
  - <eNS> is de string "ESI" of een string die op lidstaat niveau beheerd wordt.
  - <sHO> OPTIONEEL – Dit is de schacHomeOrganization, de aanduiding van de thuisinstelling van de student. Is verplicht als niet gegarandeerd kan worden dat de <code> uniek is binnen de lidstaat.
  - <code>: De code van de student die hem uniek identificeert binnen de scope (combinatie van <eNS> en <sHO>).
- Het ESI kan uitgegeven worden op het niveau van een lidstaat, instelling of onderdeel van een instelling.
- Het ESI wordt toegevoegd aan een bestaande, federatieve login flow via EduGAIN federatie.
- Het ESI wordt alleen gebruikt voor Erasmus uitwisseling.

Polymorf pseudoniem
Dit is een pseudoniem waarbij specifieke pseudoniemen voor een gebruiker worden gevormd per dienstaanbieder, zonder dat de vormende partij het specifiek pseudoniem kan herleiden of de identiteit van de gebruiker bij gebruik hoeft te kennen. De polymorfe versleuteling wordt (op termijn) toegepast bij verschillende IAA stelsels van de overheid (eHerkenning, DigiD).

1. De polymorfe versleuteling van een identifier zorgt ervoor dat alleen de dienstaanbieder de identifier kan ontsleutelen. Tijdens transport is niet vast te stellen of het dezelfde identifier betreft.
2. Het BSNk wordt gebruikt voor het transformeren van een BSN naar een Polymorfe Identiteit (PI) of Polymorf Pseudoniem (PP).
3. Door BSNk/PP kunnen private partijen binnen het eID stelsel de rol van authenticatiedienst/routeringsdienst hebben en een dienstaanbieder een BSN (PI) leveren.
4. Met een Polymorfe Pseudoniem kan een willekeurige authenticatiedienst/routeringsdienst een persistente dienst specifieke identifier (PP) leveren aan de dienstaanbieder.
5. Het polymorfe pseudoniem kan relevant zijn voor het mobiliteitsvraagstuk.

[23] https://www.surf.nl/eduid-1-digitale-identiteit-voor-studenten
[24] https://www.myacademic-id.eu/

6. Mogelijk kan het PP ook gebruikt worden bij gegevensuitwisseling tussen ketenpartijen.
7. Het gebruik heeft (technische) impact. Er wordt software beschikbaar gesteld om partijen te ontlasten.
8. Een Polymorf Pseudoniem is geen oplossing voor de matchingsvraag die ontstaat als meerdere partijen gegevens willen uitwisselen over een bepaald persoon. Hiervoor zijn nog steeds keten/sector identifiers nodig, of aanvullende afspraken rond het gebruik van Polymorf Pseudoniem en de onderlinge uitwisseling hiervan.

5.2.6. Identifiers voor niet natuurlijke personen

RIO[25]

De identiteiten van onderwijsinstellingen worden beheerd in het LAS/SIS voor vo en mbo en centraal geregistreerd in RIO. In het po gaat het beheer primair liggen in RIO en nemen de LASsen de identiteiten over in het pakket.

[25] RIO is (mogelijk) relevant voor medewerkers die namens een onderwijsaanbieder handelen

6. Architectuurkaders applicatielaag

6.1. Identiteitenbeheer

Identiteiten worden beheerd in een identiteitenbeheerdienst. De school gebruikt als identiteitenbeheerdienst voor onderwijsvolgers een LAS/SIS en een HR systeem voor onderwijsprofessionals. De identiteiten van onderwijsinstellingen worden beheerd in het LAS/SIS voor vo en mbo en centraal geregistreerd in RIO. In het po gaat het beheer primair liggen in RIO en nemen de LASsen de identiteiten over in het pakket.

6.2. Authenticatie(middelen)beheer

De applicaties binnen authenticatiemiddelenbeheer omvat functionaliteit voor:

- Beheren gegevens.
- Provisioning accounts. Vanuit een gegevensbron wordt met een interface in de voorbereidingsfase systemen voorzien van de benodigde gegevens over de digitale identiteit.
- Beheer accounts/authenticatiemiddelen

6.3. Bevoegdhedenbeheer

De applicatiedienst omvat functionaliteit voor beheren van bevoegdheden. Hierbij wordt de relatie gelegd tussen digitale identiteit toegang en de rechten op toegang. Dit omvat ook machtigen waarbij een digitale identiteit door een andere digitale identiteit is gemachtigd om iets te doen. Deze dienst legt met "regels" vast wat mag (of wat niet mag).

- Het bevoegdhedenbeheer is een functie van de Dienstaanbieder.
- Het bevoegdhedenbeheer heeft een relatie met identiteitenbeheer en authenticatiemiddelenbeheer. Gegevens binnen het identiteitenbeheer kunnen bepalend zijn voor de bevoegdheden van een dienstafnemer en provisioning zorgt ervoor dat deze gegevens aan de betreffende systemen (diensten) geleverd worden.
- In de applicatielaag worden de gegevens beheerd in een Authenticatiedienst. Afhankelijk van de context kan er provisioning nodig zijn. Met de provisioning interface kunnen andere systemen in de voorbereidingsfase voorzien worden van de benodigde informatie over de digitale identiteit.
- Machtigen wordt gezien als een onderdeel van Bevoegdhedenbeheer. Het Machtigen is echter een functie van de dienstafnemer.

6.4. Verlenen toegang

De applicatiedienst zorgt voor het verlenen van toegang en dat op het moment dat ergens toegang tot wordt gevraagd, hierbij wordt gecontroleerd of dat volgens de regels mag. De bevoegdheden kunnen grof en fijnmazig zijn en tevens generiek, dan wel specifiek per dienst. Bevoegdheden zijn hierdoor niet statisch en zullen dus wijzigen in de loop van de tijd.

7. Begrippenkader

De begrippen in dit document zijn overgenomen van de NORA en ROSA. Voor een compleet actueel beeld wordt verwezen naar de NORA[26] en ROSA[27]. Indien er geen passend begrip beschikbaar was heeft de werkgroep deze zelf geformuleerd (WG IAA)

(Dienst)Afnemer (NORA)
De persoon of organisatie die een dienst in ontvangst neemt. Dit kan een burger, een (medewerker van een) bedrijf of instelling dan wel een collega binnen de eigen of een andere organisatie zijn.

Access Management
Zie ook Bevoegdhedenbeheer en Autorisatiebeheer

Attributendienst (ROSA)
Een dienst die attributen levert op basis van de autorisatie van de partij die de gegevens ontvangt.

Authenticatie (ROSA)
Het proces om de geclaimde identiteit van een gebruiker te controleren aan de hand van een authenticatiemiddel..

Authenticatie Hub (ROSA)
Dienst die verzoeken voor gebruikersauthenticatie van dienstverleners routeert naar de authenticatiediensten van die gebruikers (dwz doorgeefluik van authenticatieverzoeken). Entree federatie en SURFConext zijn voorbeelden

Authenticatiedienst(ROSA)
Dienst die authenticatie van gebruikers aan de hand van een authenticatiemiddel uitvoert.

Authenticatiemiddel (ROSA)
Middel waarmee met (een bepaalde mate van) zekerheid de digitale identiteit van de gebruiker en/of besteller wordt vastgesteld.

Authenticatiemiddelenbeheer (NORA[28])
Beheer van authenticatiemiddelen.

Authenticiteit (NORA)
Een kwaliteitsattribuut van een informatieobject. Het toont aan dat het informatieobject is wat het beweert te zijn, dat het is gemaakt of verzonden door de persoon of organisatie die beweert het te hebben gemaakt of verzonden en dat het is gemaakt en verzonden op het tijdstip als aangegeven bij het informatieobject

Authentiek gegeven (NORA)
In een basisregistratie opgenomen gegeven dat bij wettelijk voorschrift als authentiek is aangemerkt

Autorisatie (NORA)
Het proces van het toekennen van rechten voor de toegang tot geautomatiseerde functies en/of gegevens in ICT voorzieningen

[26] https://www.noraonline.nl/wiki/Begrippenkader
[27] https://www.wikixl.nl/wiki/rosa/index.php/Begrippenlijst_ROSA
[28] NORA thema IAA is nog in ontwikkeling.
https://www.noraonline.nl/wiki/Hoe_pas_je_Identity_%26_Access_Management_toe%3F

Betrouwbaarheid (NORA)
De mate waarin de organisatie zich voor de informatievoorziening kan verlaten op een informatiesysteem. De betrouwbaarheid van een informatiesysteem is daarmee de verzamelterm voor de begrippen beschikbaarheid, integriteit en vertrouwelijkheid.

Betrouwbaarheidsniveau (eIDAS)
In deze context: de mate van zekerheid die over de identiteit van een Gebruiker gegeven kan worden bij gebruik van zijn Authenticatiemiddel. De eIDAS-verordening onderscheidt de niveaus laag, substantieel en hoog. De uitvoeringsverordening EU 2015/1502 definieert de eisen aan deze betrouwbaarheidsniveaus.

Bevoegdhedenbeheer (NORA)
De "levenscyclus" van bevoegdheden, waar vooraf wordt bepaald wat een digitale identiteit mag (of niet mag).

Dienst (NORA)
Een afgebakende prestatie van een persoon of organisatie (de dienstverlener), die voorziet in een behoefte van haar omgeving (de afnemers).

Dienstverlener / Dienstaanbieder (NORA)
De persoon of organisatie die voorziet in het leveren van een afgebakende prestatie (dienst) aan haar omgeving (de afnemers).
WG IAA toevoeging: Bij dienstverleners wordt onderscheid gemaakt tussen onderwijsinstellingen en leveranciers (diensten voor de uitvoering van 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.

Digitale Identiteit (ROSA)
Een uniek gegeven aan de hand waarvan een natuurlijk persoon of rechtspersoon in een bepaald domein gekend wordt.
Aanvulling IAA Werkgroep: Een identiteit is een set gegevens (attributen) welke tezamen specifiek kenmerkend zijn voor die ene specifieke entiteit binnen de gegeven context. Iedere entiteit (dus ook een natuurlijke persoon) heeft een oneindig aantal identiteiten omdat een identiteit een "afbeelding", een set kenmerkende gegevens over die entiteit is, die slechts zinvol is binnen de gegeven context.

Doelbinding (NORA)
Het principe dat iemand (persoon of organisatie) alleen informatie mag vragen, opslaan, gebruiken, delen ten behoeve van welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden.

Doelgroep (WG IAA)
Een doelgroep is een aanvulling op de rol Dienstafnemer en wordt gedefinieerd op basis van een aantal kenmerken waarmee deze groep zich onderscheidt van andere groepen in de context van het thema IAA. Zo kan een bepaalde doelgroep over een specifiek authenticatiemiddel beschikken, bijvoorbeeld leerlingen en studenten die over een authenticatiemiddel beschikken dat is uitgegeven door de school, of burgers die over een eID authenticatiemiddel beschikken. Een bepaald natuurlijk persoon kan tot meerdere doelgroepen behoren, het concept doelgroep wordt relevant als een natuurlijk persoon in een bepaalde rol acteert.

H2M
Uitwisseling tussen mens en een systeem typeren we als Human to Machine (H2M). Een voorbeeld hiervan gegevensuitwisseling bij bezoek van een website of gebruik van een webdienst.

IAA (Werkgroep IAA)
Identificatie, Authenticatie en Autorisatie (Zie ook Toegang en IAM).

IAM (NORA)
Identity and Access Management (IAM) is vrij vertaald het beheer om er voor te zorgen dat de juiste "identiteiten" (denk daarbij vooral aan personen of computers), voor de juiste redenen en op het juiste moment toegang krijgen tot de juiste faciliteiten. (niet vastgesteld)

Identificatie (NORA)
Het bekendmaken van de identiteit van personen, organisaties of IT-voorzieningen.

Identificeren (NORA)
Proces waarmee gebruikers op basis van een identiteitsverklaring gekoppeld worden aan een digitale identiteit met betrouwbare kenmerken. 2. Gebruik van de digitale identiteit door de gebruiker.

Identifier (WG IAA)
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. Een identifier is van een bepaald type, bijvoorbeeld transient (een dienst krijgt per sessie een andere identifier voor dezelfde entiteit), targeted (specifiek voor een bepaalde dienst), shared (dienstafnemer is bij meerdere diensten/partijen bekend onder dezelfde identifier).

Identiteitenbeheer (NORA[29])
Geeft antwoord op de vraag 'wie ben je?' (zie ook Identity Management).

Identity Management (JenV)
IdM is het registreren, verifiëren en beheren van de identiteitsgegevens en de werkrelatie van een persoon, device of softwarematig entiteit. Hieronder wordt het geheel verstaan van – al of niet geautomatiseerde – processen binnen een organisatie die betrekking hebben op deze activiteit.

M2M (UBV)
Machine to Machine (M2M) betreft de gegevensuitwisseling tussen systemen onderling. Zoals bij berichtenuitwisseling tussen partijen binnen het onderwijs. Hierbij wordt onderscheid gemaakt tussen serviceaanbieder (de partij die een dienst en/of gegevens beschikbaar stelt) en service-afnemer (de partij die een dienst gebruikt en/of gegevens ophaalt). Soms kan een partijen beide zijn, wanneer deze zowel gegevens ophaalt als beschikbaarstelt. Bijvoorbeeld in geval van Overstap Service Onderwijs (OSO).

Machtiging (NvETD)
Een herroepbare bevoegdheid die een vertegenwoordigde verleent aan een andere partij (de gemachtigde) om in naam van eerstgenoemde rechtshandelingen te verrichten.

Mandatering (ROSA)
~~Relatie tussen dienst en dienstaanbieder, gelegd door de dienstafnemer, opdat de dienstaanbieder voor deze dienst namens de dienstafnemer kan optreden. Bron: PvE Onderwijs service register~~

Natuurlijk Persoon (NvETD)
Een individueel menselijk wezen en subject van rechten en drager van plichten. Iedere natuurlijk persoon is een persoon in de zin van de hier gegeven definitie van persoon

29
https://www.noraonline.nl/wiki/Hoe_pas_je_Identity_%26_Access_Management_toe%3F

Onderwijsprofessional
De onderwijsprofessional is een medewerker bij een onderwijsorganisatie. De primaire identiteit van onderwijsprofessionals wordt bepaald binnen de context van de onderwijsorganisatie waar zij werkzaam zijn, bijvoorbeeld in de vorm van een personeelsnummer.

Onderzoeker
De onderzoeker is een onderwijsprofessional en kan dus ook als medewerker bij een onderwijsorganisatie gezien worden. Onderzoeker moeten toegang kunnen krijgen tot onderzoeksdata van andere onderzoekers.

Pseudonimisering (NORA/AVG)
Het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat aanvullende gegevens worden gebruikt, op voorwaarde dat deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld.

De uitdrukkelijke invoering van pseudonimisering genoemd in de Avg is niet bedoeld om andere gegevensbeschermingsmaatregelen uit te sluiten(AVG art. 4 lid 5). Bijzondere aspecten in dit verband zijn:

- Alle redelijke maatregelen moeten worden genomen om ervoor te zorgen dat onjuiste persoonsgegevens worden gerectificeerd of gewist(AVG overweging 39).
- De verwerkingsverantwoordelijke dient, met name met betrekking tot online-diensten en online-identificatoren, alle redelijke maatregelen te nemen om de identiteit te controleren van een betrokkene die om inzage verzoekt

Rechtspersoon / Niet natuurlijk persoon (NvETD)
Hetzij een rechtspersoon, hetzij een samenwerkingsverband van natuurlijke personen en/of niet-natuurlijke personen. Niet iedere niet natuurlijke persoon is een persoon in de zin van de hier gegeven definitie van persoon, samenwerkingsverbanden zijn namelijk verbanden van personen maar zelf geen persoon.

Routeringsvoorziening (WDO)
Met Routeringsvoorziening wordt het geheel van technische en organisatorische componenten bedoeld ter ontzorging van publieke dienstverleners, zoals bedoeld in de wet Digitale Overheid (artikel 5, lid 1, sub c).

School (ROSA)
Een onderwijsorganisatie die het verzorgen van lessen tot haar kerntaken heeft en is opgebouwd uit een bevoegd gezag en 1 of meerdere onderwijsinstellingen

Serviceregister (NORA)
Register waar overheidsorganisaties hun diensten registreren en diensten van anderen kunnen terugvinden

Toegang (ROSA)
Het Proces dat beschrijft hoe een gebruiker toegelaten kan worden tot het educatieve digitale product en in staat wordt gesteld gebruik te maken van digitaal leermateriaal.

Toepassingsgebied (NORA)
De omschrijving van het functionele gebruik van de voorziening

Vertegenwoordigde (NvETD)
De partij die de vertegenwoordiger de bevoegdheid heeft verleend om in naam van eerstgenoemde te handelen.

Vertegenwoordiger (NvETD)
De Partij die bevoegd is om een andere partij (de vertegenwoordigde) te vertegenwoordigen in het verrichten van handelingen met derden.

Vertegenwoordiging (NvETD)
De rechtsfiguur die inhoudt dat de rechtsgevolgen van een door een bepaalde Partij (de Vertegenwoordiger of Gemachtigde) in naam van een andere partij (de Vertegenwoordigde dienstafnemer) met een derde verrichte handeling aan de vertegenwoordigde worden toegerekend. De Bevoegdheid tot het verrichten van vertegenwoordigingshandelingen vloeit voort uit hetzij de wet hetzij een volmacht (privaatrecht) hetzij uit een machtiging (bestuursrecht). Zo'n bevoegdheid kan eventueel ingeperkt zijn tot bepaalde rechtshandelingen, of een bepaalde relevante omvang ten aanzien van rechtshandelingen. In privaatrechtelijke context wordt naast het begrip vertegenwoordiger, agent of gevolmachtigde gehanteerd in plaats van gemachtigde.

Verwerken (begrip gegevensmanagement)
Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

Verwerker
Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/ dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

Verwerkersovereenkomst
Hoewel de term 'verwerkersovereenkomst' in de Nederlandstalige Avg niet letterlijk wordt gebruikt, bepaalt artikel 28 toch nauwkeurig dat er een "overeenkomst of andere rechtshandeling krachtens het Unierecht of het lidstatelijke recht die de verwerker ten aanzien van de verwerkingsverantwoordelijke bindt " moet zijn, "waarin het onderwerp en de duur van de verwerking, de aard en het doel van de verwerking, het soort persoonsgegevens en de categorieën van betrokkenen en de rechten en verplichtingen van de verwerkingsverantwoordelijke worden omschreven"

Verwerkingsverantwoordelijke
Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het wettelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen. De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van lid 1 (i.e. Beginselen inzake verwerking van persoonsgegevens) en kan deze aantonen

Werkingsgebied (NORA)
Het domein (organisatorisch, taakvelden) binnen de overheid waarin het element (principe, standaard, voorziening..) wordt of kan worden toegepast. Bijvoorbeeld: gemeenten, provincies, waterschappen, Rijk, zorginstellingen, primair onderwijs.

Wettelijke vertegenwoordiging (NvETD)
Een Vertegenwoordiging (vertegenwoordigen) die voortvloeit uit de wet zonder dat er sprake is van het toekennen van een volmacht of machtiging door de Vertegenwoordigde. Voorbeelden zijn: de bestuurder(s) van een Rechtspersoon, de curator, de ouders van een minderjarige.