Visiedocument –
Digitale Identiteiten in het Onderwijs

Versie 0.6
Bedoelt voor aanscherping van openstaande punten en ter bespreking met relevante personen in het netwerk van de werkgroepleden, bijvoorbeeld collega's of sectorpartners.

Geschreven door de Edustandaard Werkgroep Toegang
9 juli 2026

1. Managementsamenvatting

Digitale identiteiten vormen de onzichtbare ruggengraat van het onderwijs. Wie toegang heeft tot welke diensten, hoe leervoortgang wordt uitgewisseld, hoe een onderwijsdeelnemer (student, leerling) zich aanmeldt bij een nieuwe school of instelling – het hangt allemaal af van hoe digitale identiteiten zijn ingericht. Het huidige stelsel werkt, maar is gebouwd rondom onderwijsorganisaties in plaats van rondom personen. Wie van onderwijsaanbieder wisselt, naar een sector overstapt of een niet-bekostigde opleiding volgt, valt buiten de bestaande voorzieningen of moet opnieuw beginnen. Dat is onhoudbaar in een wereld waarin lerenden zich steeds vaker bewegen over organisatie- en sectorgrenzen heen, en waarin digitale soevereiniteit een publieke waarde is geworden.

Het doelbeeld is een onderwijsorganisatie-overstijgend identiteitsstelsel waarin iedere onderwijsbetrokkene beschikt over een betrouwbare persoonsgebonden identiteit, regie heeft over de eigen verifieerbare verklaringen, en naadloos kan bewegen binnen het gehele onderwijsdomein – ongeacht sector, onderwijsaanbieder of levensfase.

Dit doelbeeld rust op drie bouwstenen: een betrouwbare persoonsgebonden identiteit als basis, verifieerbare verklaringen als middel om toegang en bevoegdheden te onderbouwen, en een federatief vertrouwensmodel als het kader dat interoperabiliteit en wederzijds vertrouwen borgt. Gezamenlijke governance is de randvoorwaarde die dit stelsel draaiende houdt.

De transitie naar dit doelbeeld is geen big bang maar een stapsgewijze migratie. Bestaande, wettelijk verankerde voorzieningen worden niet vervangen maar geleidelijk uitgebreid. Interoperabiliteit tussen het ECK iD en eduID is daarin een cruciaal eerste scharnierpunt. Sommige stappen kunnen nu worden gezet; andere wachten op wetgeving of Europese kaders.

Met opmerkingen [EV1]: Waarom in deze samenvatting al gelijk het eerste doel? Verderop in het stuk geven we juist meer keuzes aan. Na afloop van de meeting had ik als afdronk dat het formeel vastleggen en (wettelijk regelen) dat we gaan werken met 1 persoonsgebonden identiteit voor het hele domein de eerst opdracht is. Om daarna op basis van de verschillende scenario's de transitie te starten, Dit om rekening te houden met bijvoorbeeld het verschil tussen FO en HO etc.

Deze visie is opgesteld door de Werkgroep Toegang van Edustandaard en beoogt het gemeenschappelijke referentiekader te bieden dat de sectorarchitecturen FOSA, MOSA en HOSA met elkaar verbindt en daarmee ook de ontwikkelingen op het gebied van de digitale identiteit in de sectoren funderend onderwijs, middelbaar beroepsonderwijs en hoger onderwijs. De visie neemt bewust stelling om het gesprek in het onderwijsdomein te structureren en te versnellen.

2. Inleiding

Het onderwijs digitaliseert in hoog tempo. Onderwijsdeelnemers loggen in op leeromgevingen, docenten wisselen leervoortgang uit, onderwijsorganisaties werken samen over sectorgrenzen heen. Al die interacties veronderstellen dat bekend is wie iemand is en wat die persoon mag. Digitale identiteiten en toegang zijn daarmee geen technische bijzaak maar een strategische randvoorwaarde voor goed onderwijs.

Tegelijkertijd is het huidige stelsel van digitale identiteiten in het onderwijs gefragmenteerd gegroeid. Elke sector heeft eigen voorzieningen ontwikkeld, commerciële partijen zijn als de facto identiteitsprovider binnengeslopen, en een sectoroverstijgend referentiekader ontbreekt. De evaluatie van de Wet pseudonimisering (2024), de opkomst van eIDAS 2.0 en de Wet digitale overheid, en de ambities van de Groeifondsprogramma's Npuls en stichting Edu-V maken duidelijk dat een gemeenschappelijke visie nu urgent is.

Dit document formuleert een sectoroverstijgende architectuurvisie op digitale identiteiten in het onderwijs. Het biedt het gemeenschappelijke referentiekader dat de sectorarchitecturen FOSA, MOSA en HOSA met elkaar verbindt en daarmee het mogelijk maakt om de ontwikkelingen op het gebied van de digitale identiteit in de sectoren funderend onderwijs, middelbaar beroepsonderwijs en hoger onderwijs uit te lijnen. Dit moet de groeifondsprogramma's houvast geven bij het maken van no-regret keuzes. De visie is opgesteld door de Werkgroep Toegang van Edustandaard, onder coördinatie van OCW.

De visie richt zich op de architectuur van digitale identiteiten – de wat-vraag. De hoe-vraag, in de vorm van concrete technische oplossingen, implementatiedetails en productiekeuzes, valt buiten scope. Ook de processen die de bouwstenen ondersteunen – zoals uitgifte, machtiging en toetsing – vallen buiten de scope van deze visie. Deze horen in de uitwerking die volgt na vaststelling. De visie benoemt wallet en data als relevante context maar werkt deze niet uit; de focus ligt op identifiers en de structuur van het identiteitsstelsel. Het transitiepad wordt in hoofdlijnen geschetst in hoofdstuk 6 en uitgewerkt in een separate roadmap.

Deze visie bouwt voort op en synthetiseert een reeks bestaande architectuur- en visiestukken: de ROSA en de daarbinnen vastgestelde ontwerpkaders voor het IV-domein

IAM, de HOSA Domeinarchitectuur Identiteit en Toegang, de MOSA, de FOSA Domeinarchitectuur Digitale identiteiten, de Architectuurvisie Identiteiten en Toegang in het Hoger Onderwijs (ABHO, 2025), en het Edu-V adviesrapport opvolging aanbevelingen evaluatie Wet pseudonimisering.

Hoofdstuk 2 beschrijft wat IAM is en hoe het in het onderwijs is georganiseerd. Hoofdstuk 3 schetst de relevante ontwikkelingen die een nieuwe visie noodzakelijk maken. Hoofdstuk 4 geeft een overzicht van de huidige voorzieningen en knelpunten. Hoofdstuk 5 formuleert de visie op het toekomstige identiteitsstelsel. Hoofdstuk 6 schetst het transitiepad.

3. IAM in het onderwijs

Identity and Access Management (IAM) is het geheel van afspraken, processen en technologie waarmee geregeld wordt dat de juiste persoon – of het juiste systeem – op het juiste moment toegang krijgt tot de juiste middelen. In het onderwijs is dat geen technisch detail maar een fundamentele voorziening: studenten moeten bij hun leeromgeving kunnen, docenten bij hun toetssystemen, en instellingen moeten gegevens veilig kunnen uitwisselen. IAM raakt daarmee aan privacy, veiligheid, gebruikersgemak en digitale soevereiniteit tegelijk.

Met opmerkingen [BF2]: ik voorgaande hoofdstukken lijken we te scopen tot identiteiten die bij een persoon horen. Trekken we het hier breder? DUO lijkt daar momenteel wel naar omdat er in toenemende mate een mix ontstaat van burgers, professionals ("zakelijke klanten"), eigen medewerkers, medewerkers van collega-organisaties/ketenpartijen, applicaties, SaaS-oplossingen, agents, e.d. die toegang krijgen/zoeken.

3.1. Het belang van IAM

Goed ingericht IAM levert het onderwijs vier concrete voordelen. (1) Het zorgt voor adequate en snelle toegang: gebruikers verwachten direct bij de diensten te kunnen die ze nodig hebben, zonder onnodige drempels. (2) Het verhoogt de veiligheid: heldere en geautomatiseerde toegangsprocessen verminderen het risico op ongeautoriseerde toegang en datalekken. (3) Het maakt flexibel samenwerken mogelijk: onderwijsorganisaties, sectorpartijen en dienstverleners kunnen op basis van vertrouwensrelaties elkaars diensten benutten. (4) En het beschermt de privacy van onderwijsbetrokkenen: goede IAM-inrichting is een randvoorwaarde voor dataminimalisatie en regie op gegevens.

Omgekeerd geredeneerd brengt gebrekkig IAM concrete risico's: onduidelijk eigenaarschap over identiteiten en toegangsrechten, onnodige breedte van toegang die leidt tot extra licentiekosten, en een technische infrastructuur die moeilijk onderhoudbaar is door historische groei en fragmentatie.

3.2. IAM in het onderwijs: drie kernvragen

Om IAM in het onderwijs te begrijpen helpt het om drie fundamentele vragen te onderscheiden[1]:

Wie ben je? – Dit is de identiteitsvraag. Iedere gebruiker moet uniek en persistent bekend zijn, op een bepaald betrouwbaarheidsniveau. Een identiteit is de digitale representatie van een persoon of systeem, vastgelegd ten opzichte van een organisatie of stelsel. In het onderwijs zijn er meerdere bronnen van identiteit: van DUO-registers via eigen administraties van onderwijsorganisaties tot onderwijsorganisatie-onafhankelijke voorzieningen als eduID.nl of de Nummervoorziening. Meerdere bronnen kunnen en moeten soms naast elkaar bestaan.

Wat ben je? – Dit is de verbintenisvraag. Wat is de juridische of contractuele relatie van de gebruiker met de instelling of de keten? Een onderwijsdeelnemer heeft een

[1] Ontleend aan: Architectuurvisie Identiteiten en Toegang in het Hoger Onderwijs, versie 0.9. Werkgroep IAM – ArchitectenBeraad Hoger Onderwijs (ABHO), 25 november 2025.

inschrijving, een onderwijsmedewerker een arbeidsovereenkomst, een gastdocent een opdracht. De kwaliteit van de bronregistratie van deze verbintenis – in een SIS, LAS, HR-systeem of anderszins – is bepalend voor de betrouwbaarheid van het toegangsproces.

Wat kom je doen? – Dit is de autorisatievraag. Welke specifieke **middelen** (een applicatie, een dataset, een fysieke ruimte) heeft de gebruiker nodig voor zijn rol of taak? Dit is sterk domeinafhankelijk. De vertaling van verbintenis en rol naar concrete toegangsrechten verloopt via zogenoemde toegangspakketten – verzamelingen van rechten gecombineerd met de criteria waaraan voldaan moet worden.

Naast deze drie vragen benoemt de ROSA[2] een fundamenteel verschil tussen human-to-machine-interactie (H2M: een persoon authenticeert zich en krijgt toegang tot een dienst) en machine-to-machine-gegevensuitwisseling (M2M: een systeem krijgt toegang tot een ander systeem ten behoeve van gegevensuitwisseling). Ze komen echter wel naast elkaar en in combinatie voor, en ze gaan vaak over dezelfde betrokkene.

Met opmerkingen [BF3]: dat klopt wel, maar is opname van deze alinea wel relevant voor deze paragraaf/document?

3.3. Processen, functies en eigenaarschap

IAM bestaat uit een aantal samenhangende activiteiten. Identiteitsbeheer omvat het registreren, beheren en verwijderen van identiteiten en bijbehorende authenticatiemiddelen. Bevoegdhedenbeheer omvat het vastleggen van toegangsrechten op basis van verbintenis en rol, en het distribueren van die rechten naar systemen. Toegangsverlening omvat authenticatie – het verifiëren dat de gebruiker is wie hij zegt te zijn – en autorisatie – het beslissen of de gebruiker het gevraagde middel (bijvoorbeeld een dataset) mag gebruiken. Monitoring en beveiliging omvat logging, rapportage en controle op de juistheid van toegangsrechten.

Cruciaal is dat eigenaarschap over deze activiteiten helder belegd is. De eigenaar van een middel is verantwoordelijk voor het bepalen wie toegang mag krijgen en onder welke voorwaarden. De eigenaar van een verbintenis (zoals een inschrijving of een arbeidsovereenkomst) is verantwoordelijk voor de kwaliteit en actualiteit van de bronregistratie. Zonder helder eigenaarschap ontstaat de situatie die in het onderwijs nu veel voorkomt: toegangsrechten die niet worden ingetrokken bij uitschrijving, identiteiten die blijven bestaan na het einde van een verbintenis, en niemand die zich verantwoordelijk voelt.

Met opmerkingen [BF4]: de eigenaar moet die vaak ook nog enige tijd bewaren (archiefwet) na beëindiging van de relatie

3.4. Governance en speelveld per sector

De manier waarop IAM is georganiseerd verschilt sterk per sector – en dat verschil is een van de hoofdoorzaken van het ontbreken van een sectoroverstijgend stelsel.

---

[2] IV-domein IAM / Ontwerpgebieden Digitale identiteiten, H2M en M2M. Architectuurraad Edustandaard, vastgesteld 15 april 2025. Beschikbaar via: https://rosa.wikixl.nl/index.php/Ontwerpgebieden en https://rosa.wikixl.nl/index.php/IV-domein_IAM

In het **hoger onderwijs** bepalen instellingen grotendeels zelf hun IAM-inrichting. SURF levert sectorvoorzieningen als SURFconext en eduID, maar deelname is niet verplicht en instellingen maken eigen keuzes over identiteitsproviders en toegangssystemen. Dit leidt tot een gevarieerd maar gefragmenteerd landschap.

In het **funderend onderwijs** (po en vo) is de IAM-inrichting op schoolniveau sterk afhankelijk van leveranciers als Magister, Somtoday en Basispoort. Veel onderwijsorganisaties in het fo hebben beperkte eigen capaciteit om IAM strategisch in te richten. Kennisnet levert sectorvoorzieningen als de Entree Federatie en de Nummervoorziening voor veilige, single sign-on toegang tot diensten.

Het **mbo** zit hier tussenin: de IAM-inrichting op schoolniveau is sterk afhankelijk van leveranciers als Microsoft en Google. Er is voldoende capaciteit om de IAM in te richten, maar te weinig aandacht voor het concept sectoridentiteit. Dit zien we terug door het gebruik enerzijds van SURF-diensten (SURFconext, eduID), anderzijds sterk leunend op de Kennisnet-diensten voor SSO binnen de leermiddelenketen. De diensten van SURF en Kennisnet zijn op veel punten interoperabel, waardoor ze goed naast elkaar gebruikt kunnen worden.

Bureau Edustandaard is de sectoroverstijgende samenwerking waarin de publieke partijen (SURF, Kennisnet, MBO Digitaal, de sectorraden, OCW, DUO, Stichting Edu-V etc.) en de private partijen (brancheverenigingen van educatieve dienstverleners zoals softwareleveranciers, uitgevers en distributeurs) werken aan een gezamenlijk stelsel van afspraken en standaarden in de onderwijsketen. De Edustandaard **Werkgroep Toegang** is daarbinnen verantwoordelijk voor de architectuurkaders voor digitale identiteiten en IAM. In de praktijk is de samenwerking tussen SURF en Kennisnet echter niet altijd vanzelfsprekend, wat leidt tot bestuurlijke fragmentatie.

Met opmerkingen [EV5]: Wat bedoelen we hier nu mee? Ik denk dat het FO bij de inrichting van IAM weldegelijk zijn verantwoordelijkheid neemt. En dit ook binnen de beperkte capaciteit ook doet. Sterker nog ze schrijven leerlingen ook uit en hiermee verdwijnt deze binnen IAM omgeving. Dat dit nu niet leidt tot een signaal van de middelen wilt u deze ook opruimen is denk ik echt iets anders. Enige duiding lijkt me wel verstandig.

Met opmerkingen [EV6]: Moet deze niet apart genoemd worden bij Identiteiten of hier weglaten? want de Entree Federatie ondersteund een eenvoudige hub manier om SSO toegang te krijgen tot externe applicaties.

4. Relevante ontwikkelingen

4.1. Maatschappelijke en beleidsmatige context

Digitale soevereiniteit vormt als driver de rode draad door alle ontwikkelingen die in dit hoofdstuk worden beschreven. Zowel op gebruikersniveau – de mate waarin een persoon regie heeft over zijn eigen digitale identiteit en gegevens – als op stelselniveau – de mate waarin het onderwijs onafhankelijk is van grote commerciële platforms en niet kwetsbaar is voor vendor lock-in. IAM staat nu grotendeels onder controle van big- en medium tech, zowel aan de instellingskant (Microsoft, Google, Magister, Somtoday) als aan de gebruikerskant. De ontwikkelingen hieronder maken duidelijk waarom dit onhoudbaar is en waarom een sectoroverstijgende architectuurvisie op digitale identiteiten nu urgent is.

Leven Lang Ontwikkelen (LLO) en de flexibilisering van het onderwijs stellen als drivers nieuwe eisen aan het identiteitenstelsel. Een lerende volgt niet langer een lineaire route van po via vo naar ho, maar combineert opleidingen, wisselt van onderwijsaanbieder, volgt niet-bekostigde trajecten en beweegt over sectorgrenzen heen. Het huidige stelsel, gebouwd op onderwijsorganisatiegebonden identiteiten, kan dit niet goed faciliteren. Internationalisering versterkt dit: onderwijsdeelnemers en -medewerkers bewegen over landsgrenzen, wat vereist dat Nederlandse identiteitsvoorzieningen interoperabel zijn met Europese equivalenten.

Kunstmatige intelligentie voegt een nieuwe dimensie toe: niet alleen mensen maar ook computersystemen en AI-agents vragen toegang tot onderwijsdiensten en -gegevens. Het huidige identiteitenstelsel is hier niet op ingericht.

Achter al deze ontwikkelingen liggen primair onderwijsdoelen: toegankelijk onderwijs voor iedereen, goede begeleiding van lerenden over hun hele loopbaan, en samenwerking tussen onderwijsorganisaties. De wetgevings- en technologische ontwikkelingen zijn drijfveren, maar het onderwijs zelf is het doel.

4.2. Wetgeving die dwingt

Een reeks wettelijke ontwikkelingen maakt een herziening van het identiteitenstelsel niet alleen wenselijk maar ook verplicht.

eIDAS 2.0 is op 20 mei 2024 in werking getreden, waardoor lidstaten verplicht zijn om eind 2026 over minimaal één gratis digitale ID-wallet te beschikken. Voor Nederlandse onderwijsorganisaties en publieke dienstverleners als Studielink geldt een acceptatieplicht voor overige EU-wallets per december 2026, en voor de NL-wallet naar verwachting per voorjaar 2028. Daarnaast zijn onderwijskwalificaties, -titels en -diploma's opgenomen in de minimale attributenlijst van eIDAS 2.0, wat betekent dat deze gegevens via de wallet ontsloten moeten kunnen worden. DUO heeft hierin een rol als bronhouder. De ontwikkeling van het Nederlandse EDI-stelsel loopt echter vertraging op; het AcICT heeft recent geconstateerd dat een werkend stelsel nog ver weg is, wat de voorbereiding voor onderwijsdienstverleners bemoeilijkt.

Met opmerkingen [BF7]: is dat al vastgesteld? Of een voornemen?

De **Wet digitale overheid (Wdo)** is sinds 1 juli 2023 gefaseerd van kracht en verplicht dienstverleners om erkende inlogmiddelen te accepteren en legt een classificatieplicht op per digitale dienst. Ho-instellingen zijn aangewezen onder de Wdo via de WHW; het mbo is nog niet aangewezen. De aansluiting op het Stelsel Toegang – de toekomstige centrale voorziening die dienstverleners ontzorgt – is voor veel onderwijsorganisaties nog een open vraag.

De **Wet pseudonimisering onderwijsdeelnemers** (2017) heeft pseudonimisering van leerlinggegevens in po en vo succesvol verankerd, maar de evaluatie door KBA Nijmegen (2024) concludeert dat de wet tekortschiet in het mbo en het ho en dat zelfregulering

onvoldoende is gebleken. De aanbevelingen vragen om meer overheidsregie en een sectoroverstijgende visie.

Het **Normenkader Informatiebeveiliging** Funderend Onderwijs (IB FO, streefnorm 2030) en de **Cyberbeveiligingswet** (implementatie van NIS2) leggen aanvullende verplichtingen op rondom de beveiliging van digitale systemen en identiteiten, met name voor kritieke infrastructuur. Dit versterkt de urgentie van een robuust en goed beheerd identiteitenstelsel.

4.3. Sectorale respons

De onderwijssector heeft de afgelopen jaren een inhaalslag gemaakt met de ontwikkeling van referentie- en sectorarchitecturen. De **ROSA** biedt een ketenreferentiearchitectuur voor het gehele onderwijs met een focus op ketensamenwerking; daaronder zijn de FOSA (funderend onderwijs, Kennisnet), MOSA (mbo, MBO Digitaal) en HOSA (hoger onderwijs, SURF) ontwikkeld als doelarchitecturen voor de gewenste sectordiensten en hun voorzieningen voor de komende 5 tot 10 jaar. Alle drie bevatten een domeinarchitectuur voor identiteit en toegang, die uitgaat van een ontwikkeling van een instellingsgebonden identiteit naar een onderwijsorganisatie-overstijgende identiteit met meer regie voor de gebruiker zelf. Deze convergentie is veelbelovend, maar een sectoroverstijgend referentiekader dat de drie sectorarchitecturen met elkaar verbindt ontbreekt nog. De visie op het **Onderwijsinformatiestelsel (OIS)**, zoals vastgesteld door de Informatiekamer, biedt hiervoor een bredere, sectoroverstijgende beleidsmatige context.

De **Groeifondsprogramma's** als Npuls en Edu-V brengen aanzienlijke investeringen en momentum. Npuls (door)ontwikkelt sectorvoorzieningen voor ho en mbo, waaronder eduID, edubadges en de eduwallet-pilot. Edu-V werkt aan een afsprakenstelsel en keurmerk voor de leermiddelenketen in po, vo en mbo, met het ECK iD als verplichte identifier. Beide programma's werken aan urgente maatschappelijke vraagstukken – toegankelijkheid, privacy, veiligheid – maar doen dit zonder gemeenschappelijk referentiekader voor digitale identiteiten. Dit visiedocument beoogt dat referentiekader te bieden.

5. Huidige situatie en knelpunten

5.1. Voorzieningen

Onderstaand een overzicht van de belangrijkste **huidige voorzieningen** die een rol spelen in digitale toegang binnen het onderwijs. Het landschap is gefragmenteerd: naast bewust ontwikkelde sectorale voorzieningen zijn er talrijke oplossingen die als de facto standaard zijn gegroeid zonder dat daar een expliciete architectuurkeuze aan ten grondslag lag.

Het onderwijs kent een bestaand **federatief stelsel** waarin partijen elkaar **vertrouwen** voor authenticatie en toegang. Dit stelsel bestaat uit meerdere **lagen**: (1) identiteiten, identifiers en pseudoniemen die bepalen wie iemand is, (2) identificatiemiddelen voor authenticatiefuncties en identiteitsproviders die dat bewijzen, (3) federaties die onderwijsorganisaties en diensten met elkaar verbinden via single sign-on (SSO), en (4) ketenkoppelingsstandaarden die de gegevensuitwisseling tussen computersystemen regelen. Daarnaast zijn er (5) registers, (6) voorzieningen voor aanmelding en inschrijving en opkomende voorzieningen voor (7) verifieerbare verklaringen (verifiable credentials) en wallets.

5.1.1. Identiteiten, identifiers en pseudoniemen

Het *persoonsgebonden nummer (PGN)* – in de praktijk het BSN, of een door DUO toegekend onderwijsnummer – is de wettelijke grondslag voor identificatie van elke onderwijsdeelnemer. Het PGN wordt beheerd door DUO en is de bron waaruit pseudoniemen kunnen worden afgeleid. Het is sectorbreed en volwassen.

Het *ECK iD* is een ketenpseudoniem dat door de Nummervoorziening van Kennisnet wordt gegenereerd op basis van het PGN. Het is sectorgebonden (po, vo, mbo) en bedoeld voor gebruik in de leermiddelenketen, zowel voor machine-to-machine communicatie als voor identificatie in het H2M-proces. In po en vo is het ECK iD volwassen en grotendeels geïmplementeerd. In het mbo is de implementatie onvolledig, mede door historische en technische belemmeringen. In het ho wordt het ECK iD niet gebruikt. Met privacy als uitgangspunt is bewust gekozen om geen sectoroverstijgend ECK iD aan te maken. Dit bemoeilijkt echter sectoroverstijgend onderwijs.

Het *instellingsgebonden studentnummer* (ho) is een door de instelling zelf toegekend nummer, doorgaans gebaseerd op de aanmelding via Studielink. Het is niet persistent over instellingen heen en kent geen sectorale standaard. Volwassen maar gefragmenteerd.

5.1.2. Authenticatiemiddelen en identiteitsproviders

DigiD is het rijksbrede identificatiemiddel voor burgers en daarmee de toegangspoort tot onder meer Studielink en DUO-diensten. Naast DigiD zijn ook gecertificeerde Europese identificatiemiddelen toegestaan op grond van eIDAS 2.0. Volwassen, sectorbreed relevant, maar niet ontworpen voor het dagelijks gebruik binnen onderwijsorganisaties.

eduID is een door SURF beheerde, instellingsonafhankelijke digitale identiteit, primair gericht op mbo, ho en wo. De gebruiker maakt het zelf aan; het is levenslang geldig en de gebruiker heeft er regie over. EduID heeft veel potentie – met name als persistente identifier voor LLO en sectoroverstijgend onderwijs – maar is nog in ontwikkeling. Een wettelijke grondslag voor de identifier-functie ontbreekt vooralsnog (WHW-aanpassing in verkenning met OCW).

Microsoft, Google, Magister en Somtoday fungeren in de praktijk als de facto identiteitsproviders binnen veel onderwijsorganisaties. Dit is geen bewuste architectuurkeuze maar een gevolg van het ontbreken van publieke sectorale alternatieven. De uitgifte en het beheer van digitale identiteiten zijn daarmee in te grote mate in handen van commerciële partijen, wat een risico vormt voor digitale soevereiniteit en publieke regie op het identiteitsstelsel.

5.1.3. Federaties

SURFconext is de federatieve toegangsinfrastructuur voor ho, wo en deels mbo, beheerd door SURF. Volwassen en breed gedragen. Instellingen zijn aangesloten als identiteitsprovider; dienstverleners als serviceprovider. Knelpunt: instellingsgebonden identiteiten blijven de basis, waardoor instellingsonafhankelijk gebruik beperkt is.

Kennisnet Federatie (Entree) vervult een vergelijkbare rol voor po, vo en mbo. Volwassen in po en vo. Knelpunt: de federatie is afhankelijk van de kwaliteit van de onderliggende identiteitsproviders per onderwijsorganisatie, die sterk varieert.

Basispoort is een toegangsdienst specifiek voor po, beheerd door een private dienstverlener. Breed gebruikt maar niet ontworpen als sectorale basisinfrastructuur. De dienst vormt een afhankelijkheid buiten de publieke governance.

5.1.4. Ketenkoppeling

De *Nummervoorziening* van Kennisnet verzorgt de pseudonimisering van het PGN naar het ECK iD. Volwassen in po/vo, onvolledig in mbo.

Edukoppeling is de standaard voor beveiligde gegevensuitwisseling in de onderwijsketen, beheerd door Kennisnet/Edustandaard. Sectorbreed, volwassen.

OEAPI is een opkomende standaard voor gestandaardiseerde uitwisseling van onderwijsdata tussen onderwijsorganisaties en diensten, met name relevant voor ho en mbo. OEAPI-diensten vereisen dat de afnemende partij geauthenticeerd en geautoriseerd is met gebruikmaking van OAuth, waardoor de keuzes in het identiteitenstelsel bepalend zijn voor wat via OEAPI ontsloten kan worden. Nog in ontwikkeling, veel potentie.

Het Edu-V-afsprakenstelsel biedt al een standaard waarmee onderwijsdata op een gestandaardiseerde manier kunnen worden uitgewisseld tussen onderwijsorganisaties en diensten, inclusief bijbehorende governanceafspraken. Dit is met name relevant voor het primair en voortgezet onderwijs. De standaard vereist dat de afnemende partij wordt geauthenticeerd en geautoriseerd met behulp van OAuth. Een deel is al in productie; enkele ketenprocessen zijn nog in ontwikkeling.

5.1.5. Registers

DUO beheert de centrale registers die de grondslag vormen voor digitale identiteiten in het onderwijs. In het *Register Instellingen en Opleidingen (RIO)* wordt enerzijds (door

onderwijsorganisaties zelf) vastgelegd welke onderwijsorganisaties en opleidingen er zijn (onderwijsinrichting) en anderzijds welke erkend zijn (onderwijserkenningen) door een onderwijserkenner (veelal is dat de overheid c.q. OCW); het Register Onderwijsdeelnemers (ROD) registreert de inschrijvingen en resultaten van alle onderwijsdeelnemers in het onderwijs. Beide registers vormen de gezaghebbende bron voor de verbintenis tussen een onderwijsdeelnemer en een onderwijsaanbieder en een onderwijsinstellingserkenning – de "wat ben je"-vraag uit sectie 2b.

Daarnaast beheert DUO het *persoonsgebonden nummer* (PGN), de wettelijke grondslag voor identificatie van iedere onderwijsdeelnemer, en is DUO aangewezen als bronhouder voor onderwijskwalificaties, -titels en -diploma's onder eIDAS 2.0. In het toekomstige identiteitsstelsel krijgt DUO daarmee een prominentere rol: niet alleen als beheerder van de bron waaruit pseudoniemen worden afgeleid, maar ook als uitgever van verifieerbare verklaringen over onderwijsresultaten die via de wallet kunnen worden ontsloten.

5.1.6. Aanmelding en inschrijving

Met opmerkingen [EV8]: Moet er nog iets worden toegevoegd over het aanmeldproces binnen po en vo en de wettelijke taak die de school hierbij heeft. Wat juist deze sectoren vragen bij de uitwerking van het wat om een andere inkleuring van de architectuurvisie.

Studielink (ho) en *Cambo* (mbo) zijn de sectorale aanmeld- en inschrijfvoorzieningen. Bij aanmelding verifieert Studielink de identiteit van de aanmelder via het BSN, dat wordt opgehaald uit de DUO-registers. Dit maakt Studielink tot het eerste moment waarop een digitale identiteit in het ho wordt aangemaakt of gekoppeld aan een bestaande bronidentiteit. De inschrijvingsgegevens die Studielink vervolgens aanlevert aan instellingen vormen de basis voor de juridische verbintenis – en daarmee voor de toegangsrechten die de student krijgt. Binnen het Npuls-programma AII wordt een nieuwe voorziening ontwikkeld die Studielink op termijn vervangt en voornemens is om Cambo te vervangen. Beide voorzieningen moeten onder de Wet digitale overheid aansluiten op het Stelsel Toegang.

5.1.7. Credentials en wallet

Edubadges is een door SURF beheerde voorziening voor het uitgeven van digitale micro-credentials op basis van open standaarden. Actief in ho en mbo, groeiend. Potentie als bouwblok voor de wallet.

Eduwallet is een door Npuls gefinancierde pilot voor een persoonlijke digitale portemonnee met verifieerbare credentials (eduID, edubadges, diploma's). Nog in pilot-fase, maar strategisch het meest vergaande initiatief richting self-sovereign identity in het onderwijs.

5.2. Knelpunten

Het huidige federatieve stelsel werkt: gebruikers kunnen inloggen, diensten zijn toegankelijk, en pseudonimisering beschermt de privacy van leerlingen in de leermiddelenketen. Toch zijn er structurele knelpunten die een sectoroverstijgende visie noodzakelijk maken.

Het stelsel is gebouwd op basis van de instellingserkenningen die binnen een onderwijsorganisaties vallen (wat in het geval van het funderend onderwijs vaak te grofmazig is), niet rondom personen. Identiteiten zijn gekoppeld aan een onderwijsaanbieder (eigenlijk aan de instellingserkenning en soms de vestigingserkenning) – wie van onderwijsaanbieder wisselt, naar een andere sector overstapt of een niet-bekostigde opleiding volgt, valt buiten de bestaande voorzieningen of moet opnieuw beginnen. Dat hindert het streven naar Leven Lang Ontwikkelen structureel.

Daarnaast heeft de gebruiker weinig controle over diens eigen digitale identiteit en gegevens. Tegelijkertijd is er een omvangrijk schaduwsysteem van parallelle identifiers ontstaan – een gevolg van het ontbreken van sturing en volledige dekking van de officiële voorzieningen – dat de fragmentatie vergroot en de beheerbaarheid en veiligheid van het stelsel ondermijnt. De afhankelijkheid van commerciële identiteitsproviders buiten publieke governance versterkt dit verder.

Een aanvullend knelpunt is het ontbreken van een gedeeld vertrouwensmodel. Partijen weten niet altijd of een verklaring of identiteit betrouwbaar is, wie bevoegd is die uit te geven, en of de gehanteerde standaarden compatibel zijn. Dit maakt het moeilijk om op elkaar te vertrouwen zonder steeds terug te vallen op centrale tussenschakels.

5.3. Perspectief van de verschillende sectoren

Volgt na discussie met de hele werkgroep Toegang.

6. Een sectoroverstijgend identiteitsstelsel voor het onderwijs

Het huidige identiteitsstelsel is gebouwd rondom instellingserkenningen waaronder een of meerdere onderwijsaanbieders worden erkend. Wie van onderwijsaanbieder wisselt (en daarmee ook vaak wisselt van instellingserkenning), naar een andere sector overstapt of een niet-bekostigde opleiding volgt, verliest zijn digitale identiteit of moet opnieuw beginnen. Dat is onhoudbaar in een wereld waarin lerenden zich steeds vaker bewegen over organisatie- en sectorgrenzen heen, en waarin digitale soevereiniteit – zowel voor individuen als voor de sector als geheel – een publieke waarde is geworden.

Deze visie beschrijft het doelbeeld: een onderwijsorganisatie-overstijgend identiteitsstelsel waarin de onderwijsbetrokkene autonoom kan handelen, regie heeft over de eigen digitale identiteiten en naadloos kan bewegen binnen het onderwijsecosysteem. Dat doelbeeld rust op drie bouwstenen: een betrouwbare persoonsgebonden identiteit, verifieerbare verklaringen, en federatief vertrouwensstelsel. Samen maken zij een hybride stelsel mogelijk waarin het bestaande

Met opmerkingen [EV9]: Ben niet de expert maar klopt dit ook voor het FO? Krijgt elke leerling bij een inschrijving en bij een overstap naar een andere school binnen dezelfde sector steeds een nieuwe PGN?
En moeten we niet iets gezegd worden over het Eck-iD die als pseudoniem op de identiteit een probleem de leermiddelenketen heeft opgelost maar wettelijk niet schaalbaar is.

Met opmerkingen [Md10R9]: Vraag aan Brian: klopt de beschrijving van PGN en ECK iD in het fo? Krijgt een leerling bij elke overgang naar een andere school een nieuw ECK iD, of alleen bij sectorovergang? En wat moet er meer worden gezegd over de wettelijke reikwijdte van het ECK iD?

federatieve model stapsgewijs wordt uitgebreid – zonder bestaande ketens te ontwrichten.

De kaders en ontwerpprincipes hieronder leggen het normatieve fundament voor dit stelsel.

6.1. Kaders

De visie op digitale identiteiten in het onderwijs bouwt voort op de architectuurkaders (kernwaarden, kwaliteitsdoelen, architectuur- en ontwerpprincipes en ontwerpkaders) die in de ROSA zijn opgenomen en in de Edustandaard Architectuurraad zijn vastgesteld voor het ontwerpgebied Digitale identiteiten en het IV-domein IAM. Waar deze visie vooruitloopt op de huidige praktijk, verankeren we die in architectuurkaders die al in de ROSA zijn opgenomen maar waarvan de reikwijdte in het beoogde stelsel wordt vergroot. Twee overkoepelende kernwaarden kleuren alle principes die volgen.

Het eerste is **autonomie**[3]. Waar de huidige doelarchitecturen van het onderwijs (HOSA, MOSA en FOSA) vergelijkbare doelen nastreven, beogen we in deze visie een stap verder te gaan: een onderwijsbetrokkene moet in staat worden gesteld autonoom te handelen binnen het digitale onderwijsdomein.

Het tweede is de kernwaarde **rechtvaardigheid**[4] en daarbinnen dan met name het kwaliteitsdoel **inclusiviteit**[5]. Er mogen geen nieuwe drempels worden opgeworpen voor deelname aan onderwijs of digitale dienstverlening. Niet iedere onderwijsbetrokkene beschikt over dezelfde digitale vaardigheden, middelen of mogelijkheden. Leerlingen in het primair onderwijs zijn niet altijd handelingsbekwaam; in het voortgezet onderwijs wordt het gebruik van een smartphone steeds meer aan banden gelegd – het meest voor de hand liggende dragermedium voor moderne identiteitsapplicaties. Inclusiviteit stelt daarom eisen aan gebruiksvriendelijkheid, governance, toegankelijkheid, vertegenwoordiging en de beschikbaarheid van publieke en laagdrempelige voorzieningen.

6.2. Ontwerpprincipes

1. Iedere onderwijsbetrokkene heeft een digitale identiteit

Iedere entiteit (persoon, organisatie) of apparaat (computerprogramma, applicatie) in het onderwijsdomein beschikt over ten minste één digitale identiteit. Dit geldt voor onderwijsdeelnemers, medewerkers en externe begeleiders, maar ook voor onderwijsorganisaties zelf en de apparaten waarmee zij werken. Het identiteitsstelsel mag geen beperkingen opleggen die bepaalde groepen onnodig benadelen of uitsluiten. Dat stelt aanvullende eisen aan het stelsel voor groepen die niet via conventionele

[3] Autonomie: https://rosa.wikixl.nl/index.php/Id-d7d22b04cc96425297de4a21ddf22939
[4] Rechtvaardigheid: https://rosa.wikixl.nl/index.php/Id-cef3416a170943c1a86a53d3c251d3fd
[5] Inclusiviteit: https://rosa.wikixl.nl/index.php/Id-aa6bd177e1cb4e699facb3ea5ddffafd

middelen kunnen participeren, waaronder jonge leerlingen, mensen met beperkingen en mensen zonder adequate digitale middelen.

2. De digitale identiteit is contextspecifiek

Een onderwijsbetrokkene kan in het onderwijs meerdere rollen en contexten hebben: onderwijsdeelnemer, ouder, onderwijsprofessional. De digitale identiteit die in een bepaalde context wordt gebruikt is specifiek voor die context; een digitale identiteit kan daarmee meerdere contexten tegelijk hebben. De context bepaalt welke attributen worden gedeeld. Onnodige koppelingen tussen contexten worden vermeden.

3. Gelaagd identiteitsmodel: bronidentiteit en functionele identiteiten

De digitale identiteiten in het onderwijsdomein zijn gelaagd opgebouwd. Een betrouwbare persoonsgebonden bronidentiteit – aangeboden vanuit het publieke domein – vormt de basis. Daarop worden contextspecifieke functionele identiteiten gebaseerd die passend zijn voor de beoogde context. Attributen in functionele identiteiten die één-op-één overeenkomen met de bronidentiteit dienen actueel en consistent te blijven. Hiervoor moet de afhankelijkheid tussen identiteiten expliciet gedefinieerd en beheerd worden. In een gelaagd identiteitsmodel, waarbij attributen een directe afhankelijkheid hebben met een bronidentiteit, ontstaat de noodzaak om met attribute-assurance te werken waarbij de zekerheid van een individueel attribuut wordt vastgelegd.

4. Betrouwbaarheidsniveau passend bij de toepassing

Niet iedere toepassing vereist dezelfde mate van zekerheid over de identiteit van een persoon. Betrouwbaarheidsniveau gaat over de mate van zekerheid dat de geclaimde identiteit behoort tot de persoon (identity-assurance); het zegt niet iets over de zekerheid van alle individuele attributen van de identiteit (attribute-assurance)[6]. Het vereiste betrouwbaarheidsniveau wordt bepaald door wat de gebruiker komt doen – het specifieke proces en de bijbehorende risico's. Een dienst die toegang geeft tot gevoelige persoonsgegevens vereist een hoger betrouwbaarheidsniveau dan een dienst die alleen publiek beschikbare informatie ontsluit. Het stelsel ondersteunt meerdere betrouwbaarheidsniveaus naast elkaar. Het identiteitsstelsel voorkomt dat een hoger betrouwbaarheidsniveau wordt gevraagd dan nodig.

5. Toegang is gebaseerd op verifieerbare verklaringen van vertrouwde partijen

Toegang tot digitale diensten wordt verleend op basis van verifieerbare verklaringen die afkomstig zijn van vertrouwde partijen. Vertrouwende partijen baseren hun vertrouwen op de betrouwbaarheid van de verklaring, de geldigheid en de verstrekker ervan. Het stelsel maakt het mogelijk verklaringen bij meerdere verklarende partijen op te halen en te combineren.

[6] https://ec.europa.eu/digital-building-blocks/sites/spaces/DIGITAL/pages/467110081/eIDAS+Levels+of+Assurance

Met opmerkingen [EV11]: ehh mijn afdronk was 1 persoonlijke identiteit die zodra deze binnen een context gebruikt wordt eventueel omgezet wordt naar een contextid (eck-id) aangevuld met attributen etc,

Anders snap ik punt 1 niet. En daarmee ook niet het centrale probleem

NB bij 3 staat eigenlijk wat ik bedoel. Maar dan snap ik misschien toch niet wat we met 2 bedoelen.

Met opmerkingen [PL12]: 'Context' kan een enkele interactie zijn, maar ook het hele stelsel. Gaat er om wat je in een bepaalde context mag en moet gebruiken. Ene uiterste is een betekenisloos eenmalig pseudoniem, andere uiterste is een persistent nummer a la BSN.

Met opmerkingen [PL13R12]: Identiteit != authenticatie

Met opmerkingen [PL14R12]: Authenticatie is in essentie het omzetten van een set identificerende attributen van de persoon naar een in de context van de ontvanger bruikbare en toegestane identiteit.

Met opmerkingen [hp15]: Willen we hier niet ook iets opschrijven hoe scholen tot een betrouwbare identiteit komen (aanmeld en registratieproces icm DUO) en bepalen welke functies deze identiteit krijgt?

Met opmerkingen [DG16]: Bij toepassing van eIDAS level of assurance: Zou bij een gelaagd identiteitsmodel met contextuele attributen attribute-assurance per attribuut nog een toegevoegde waarde hebben? Het kan ook zijn dat één niveau van assurance voor alle attributen (waarbij de zwakste schakel geldt?) ook voldoet.

Daar lijken we hier namelijk wel op voor te sorteren in ontwerpprincipe 3. Zo ja, dan zou ik opnemen:
“In een gelaagd identiteitsmodel, waarbij attributen een directe afhankelijkheid hebben een bronidentiteit, ontstaat de noodzaak om met attribute-assurance te werken waarbij de zekerheid van een individueel attribuut wordt vastgelegd.”

6. **Dataminimalisatie en doelbinding**

Verwerking van persoonsgegevens wordt beperkt tot wat noodzakelijk is voor het beoogde doel. Attributen in een identiteitsverklaring worden beperkt tot wat de context of dienst vereist; dit bepaalt in grote mate wat de gebruikscontexten (zie principe 3) kunnen en mogen zijn. Verstrekkers van attributen weten niet voor welke dienst de verklaring wordt gebruikt. Gebruikers kunnen – afhankelijk van wat de context of dienst vereist – anoniem, pseudoniem of met een bekende identiteit toegang krijgen. Een beperkte verklaring die afdoende is voor een proces vervangt het verstrekken van bredere persoonsgegevens.

Met opmerkingen [EV17]: Lopen we hier nu het risico dat binnen de onderwijscontext tijdens de SSO flow weer enorm veel context gerichte attributen over de lijn gaan? Terwijl juist binnen po en vo dankzij het eck-id we juist een knip hebben gelegd tussen H2M wat heb je dan nodig om authenticatie en basis autorisatie te kunnen doen om dan op basis van een M2M koppeling de noodzakelijke context gericht aanvullende attributen uit te wisselen dit op basis van afgesproken transactie standaarden. Hoop doel is om binnen SSO Entree Federatie uiteindelijk een minimale ARP te krijgen.

7. **Eigen regie van de onderwijsbetrokkene**

Een onderwijsbetrokkene wordt in staat gesteld regie te voeren over de eigen digitale identiteiten. Dit omvat controle over welke gegevens worden gedeeld, met wie en voor welk doel. Het stelsel maakt duidelijk waar een onderwijsbetrokkene wel en niet regie over kan voeren en waarom; in het verlengde daarvan: waar een onderwijsbetrokkene regie over kan laten voeren door een ander persoon. Waar bijvoorbeeld een persoon niet in staat is zelf regie te voeren – zoals bij jonge leerlingen of mensen met ondersteuningsbehoeften – wordt vertegenwoordiging gefaciliteerd.

Een bijzondere vorm van vertegenwoordiging is mandatering: een onderwijsbetrokkene kan een andere persoon of organisatie machtigen om namens hem of haar te handelen. In het funderend onderwijs heeft de school bovendien een wettelijke taak waarbij zij een gedelegeerde rol vervult ten aanzien van de onderwijsidentiteit van leerlingen, inclusief welke gegevens worden gedeeld.

8. **Publieke regie en leveranciersonafhankelijkheid**

Het identiteitsstelsel is gebaseerd op open standaarden en publieke governance. Onderwijsorganisaties bepalen in gezamenlijkheid welke standaarden worden gebruikt, welke publieke voorzieningen daarbij gebruikt moeten worden, hoe governance wordt ingericht en hoe publieke waarden worden geborgd. Publieke waarden, zoals digitale soevereiniteit, binnen het onderwijs vereisen dat publieke open voorzieningen gerealiseerd en gebruikt gaan worden voor de bouwstenen. Dit vermindert de afhankelijkheid van publieke en private dienstverleners en maakt het beoogde identiteitsstelsel een bouwsteen voor het Nederlandse OIS, zoals gedefinieerd door de Informatiekamer.

6.3. Bouwsteen 1: Betrouwbare persoonsgebonden identiteit

De basis van het toekomstige identiteitsstelsel is een betrouwbare persoonsgebonden identiteit – ook wel foundational identity genoemd. Dit is een identiteit die is verankerd in het publieke domein, doorgaans bij de overheid, en die de persoon als burger of inwoner uniek identificeert. Het identiteitsstelsel ondersteunt identiteiten voor Nederlandse, Europese en niet-Europese personen. In Nederland vormt het BSN de grondslag voor deze bronidentiteit; op Europees niveau biedt eIDAS 2.0 het kader voor

grensoverschrijdende erkenning. Op internationaal (niet-Europees) niveau is een grondslag of kader (nog) niet duidelijk en bieden digitale paspoortscans (binnen het ho) slechts een beperkt betrouwbaarheidsniveau.

De persoonsgebonden identiteit wordt meestal gegenereerd tijdens de onboarding in het onderwijs. Het identiteitsmodel kent drie lagen. De eerste is de **foundational identity** – de wettelijk verankerde bronidentiteit van de persoon als burger, verankerd in het publieke domein. De tweede is de **onderwijsidentiteit** – een sectoroverstijgende stamidentiteit die eenmalig wordt aangemaakt bij instroming in het onderwijs, afgeleid van de foundational identity via een onboardingsproces. Dit is een digitale identiteit in publiek beheer, vergelijkbaar met wat eduID beoogt te zijn. De derde laag zijn de **contextspecifieke identiteiten en pseudoniemen** – per onderwijsorganisatie of keten afgeleid van de onderwijsidentiteit. Het ECK iD is een voorbeeld van zo'n contextspecifiek pseudoniem.

Waar de onboarding plaatsvindt kan verschillen: een kind dat wordt aangemeld door een ouder bij een basisschool, een Nederlandse, Europese of niet-Europese student die zich inschrijft bij een Nederlandse hogeschool, een burger die solliciteert bij een onderwijsorganisatie – in elk geval doorloopt de betrokkene een onboardingsproces waarbij de foundational identity de basis vormt voor de onderwijsidentiteit. Over het algemeen is dit onboardingsproces eenmalig. Een medewerker van de ene onderwijsorganisatie die zich aanmeldt voor een opleiding bij een andere, hoeft niet opnieuw door dit proces: beide organisaties koppelen aan dezelfde onderwijsidentiteit de verklaringen die nodig zijn voor de betreffende rol.

Een onderwijsbetrokkene kan tegelijkertijd leerling, student, medewerker, ouder of gast zijn. Elke rol brengt andere bevoegdheden, rechten en relaties met zich mee. De functionele identiteit die in een bepaalde context wordt gebruikt is specifiek voor die context – onnodige koppelingen tussen contexten worden vermeden. Attributen die één-op-één overeenkomen met de bronidentiteit dienen actueel en consistent te blijven; de afhankelijkheid tussen identiteiten moet expliciet worden gedefinieerd en beheerd.

De persoonlijke identiteitsomgeving – waarvan een wallet een mogelijke technische implementatie is – is de plek waar de bronidentiteit en de daarop gebaseerde verklaringen worden beheerd. De visie gaat uit van een identiteitslandschap dat niet bestaat uit één centrale voorziening, maar uit meerdere samenhangende identiteitsdomeinen die functioneren binnen een gedeeld vertrouwensstelsel.

6.4. Bouwsteen 2: Verifieerbare verklaringen

Waar bouwsteen 1 bepaalt wie iemand is, worden verifieerbare verklaringen gebruikt om te bepalen wat iemand mag – op basis van wat een vertrouwde partij over die persoon heeft vastgesteld. Een verifieerbare verklaring is een digitaal bewijs, uitgegeven door een

bronhouder, dat door de ontvanger cryptografisch kan worden geverifieerd zonder dat de bronhouder daarbij betrokken hoeft te zijn. De onderwijsbetrokkene beheert deze verklaringen in de eigen persoonlijke identiteitsomgeving en deelt ze gericht – alleen wat nodig is, alleen met wie het nodig is.

Daarbij is het van belang onderscheid te maken tussen identiteitsverklaringen – die bewijzen wie iemand is – en authenticatieverklaringen – die bewijzen dat iemand op dit moment aanwezig is en toestemming geeft. Beide zijn verifieerbare verklaringen maar dienen verschillende doelen en kennen verschillende uitgifte- en verificatieprocessen.

Waar een onderwijsbetrokkene niet zelf in staat is verklaringen te beheren of te delen – zoals bij jonge leerlingen – kan een gemachtigde partij, zoals een ouder of de school, namens hem of haar handelen. Een dergelijk mandaat is zelf ook een verifieerbare verklaring: de gemachtigde kan aantonen bevoegd te zijn om namens de betrokkene op te treden.

In vrijwel alle contexten binnen het onderwijs bestaan toepassingen voor verifieerbare verklaringen. Bij aanmelding en inschrijving kunnen verklaringen worden gebruikt voor identiteitsvaststelling, vooropleidingen en bevoegdheden. Bij diplomering ontstaan digitale diploma's en certificaten die door individuen gecontroleerd gedeeld kunnen worden – ook buiten het onderwijsdomein, bijvoorbeeld richting de arbeidsmarkt. Binnen het speciaal onderwijs bewegen ambulante begeleiders en samenwerkingsverbanden zich regelmatig over grenzen van scholen, besturen en ondersteuningsorganisaties heen; verifieerbare verklaringen maken het mogelijk om gedurende beperkte tijd toegang te verlenen tot specifieke gegevens of begeleidingsinformatie rondom een leerling.

Deze scenario's laten zien dat er een brede behoefte bestaat aan interoperabele, gestandaardiseerde verifieerbare verklaringen – binnen het onderwijsdomein en daarbuiten. Standaardisatie betreft niet alleen techniek, maar ook semantiek en processen. Alleen wanneer organisaties overeenstemming hebben over de betekenis, governance en het gebruik van verklaringen kan een betrouwbaar en interoperabel identiteitsstelsel ontstaan. Daarbij is essentieel dat verschillende toepassingscontexten van elkaar worden onderscheiden: het uitgeven van een identiteitsverklaring vereist andere processen en waarborgen dan het uitgeven van een diploma. Verifieerbare verklaringen moeten bovendien altijd verifieerbaar blijven – bevoegdheden kunnen in de tijd veranderen en verklaringen mogen geen eigen leven gaan leiden.

6.5. Bouwsteen 3: Federatief vertrouwensmodel

Het toekomstige identiteitsstelsel is geen vervanging van het bestaande federatieve model – het is een uitbreiding ervan. De federatie blijft onmisbaar, maar krijgt een andere rol. Waar de federatie nu fungeert als centrale hub die bij vrijwel alle authenticatie-interacties betrokken is, verschuift een deel van die interacties naar directe uitwisseling van verifieerbare verklaringen tussen bronhouder, persoonlijke identiteitsomgeving en

Met opmerkingen [PL18]: Het gaat hier om zowel vertrouwen op organisatorisch niveau (wie vertrouwt wie) als op technisch niveau (hoe bewijs je het vertrouwen)

Met opmerkingen [Md19R18]: Waar precies wil je deze tekst toevoegen?

Met opmerkingen [EV20]: Hoe gaan we dan om met de verschuiving waarbij juist de IAM van de onderwijsorganisatie steeds meer op basis van SSO direct inlogt bij een middel? Denk aan office365 en Google.

ontvangende partij. De onderliggende cryptografische technieken zorgen ervoor dat deze uitwisseling doelgericht is en privacy beter kan worden geborgd: een organisatie ontvangt niet langer meer persoonsgegevens dan nodig is voor het betreffende proces.

De federatie blijft echter het fundament voor governance, interoperabiliteit, semantische afspraken en wederzijds vertrouwen tussen partijen. Zonder een federatief vertrouwenskader weten partijen niet of een verklaring betrouwbaar is, wie bevoegd is die uit te geven, en of de standaarden die worden gehanteerd compatibel zijn. De federatie is daarmee de lijm die de drie bouwstenen bij elkaar houdt.

Het resultaat is een hybride stelsel: het federatieve model en de directe verificatie van verklaringen bestaan naast elkaar en versterken elkaar. Onderwijsorganisaties, dienstverleners en afnemers met hun gebruikers kunnen stapsgewijs toewerken naar meer directe uitwisseling, zonder dat bestaande ketens worden ontwricht. De technische interacties binnen het identiteitsstelsel worden daarmee breder en beter gedistribueerd dan in de huidige situatie – maar altijd binnen de kaders die de federatie stelt.

Een cruciaal eerste scharnierpunt in dit hybride stelsel is de interoperabiliteit tussen het ECK iD en eduID. Beide voorzieningen bedienen nu verschillende sectoren en doelgroepen, maar samen dekken ze het grootste deel van het onderwijsdomein. Door ze interoperabel te maken ontstaat een no-regret stap die de drempel voor alle sectoren en daarbinnen vallende werkingsgebieden verlaagt en het grootste netwerkeffect genereert: wie aansluit profiteert direct van wat al is opgebouwd in de andere sector.

6.6. Gezamenlijke governance

De ontwikkeling naar een gedistribueerd identiteitsstelsel vermindert de verantwoordelijkheid van onderwijsorganisaties niet – het vergroot die juist. Ook in een landschap waarin individuen meer autonoom kunnen handelen en verklaringen direct kunnen delen, moeten onderwijsorganisaties regie kunnen voeren over de digitale identiteiten die onder hun verantwoording vallen. Zij blijven, mede vanuit IBP-kaders, verantwoordelijk voor lifecyclemanagement, de uitgifte van verklaringen, de inrichting van toegang en governance op gegevensuitwisseling. Rollen en rechten moeten gecontroleerd worden verstrekt, gewijzigd en ingetrokken op basis van actuele onderwijsrelaties.

Dit vereist gezamenlijke afspraken. Het toekomstige identiteitsstelsel kan alleen functioneren wanneer organisaties overeenstemming bereiken over interoperabiliteit, betrouwbaarheidsniveaus en vertrouwensmodellen. Dat geldt voor alle bronhouders en ontvangende partijen binnen het stelsel. Onderwijsorganisaties moeten gezamenlijk kunnen bepalen welke standaarden worden gebruikt, welke publieke voorzieningen nodig zijn, hoe governance wordt ingericht, welke publieke waarden worden geborgd en hoe de autonomie van onderwijsbetrokkenen wordt beschermd. Goed gekozen

Met opmerkingen [EV21]: Ik vraag me af of dit niet een aparte paragraaf waardig is. Want het staat wat mij betreft los van het federatieve stelsel. Het gaat om een identiteit van een persoon binnen een huidige context. Met de kanttekening dat we het 1 persoonlijke unieke sector overstijgende identiteit dan nog niet op hebben gelost. Plus het is voor mij geen WAT meer maar een soort van HOE.

Met opmerkingen [hp22]: Kunnen we hier concreter worden in het advies? Moet OCW niet als opdrachtgever functioneren en bijvoorbeeld Kennisnet, Surf en Edu-V aanwijzen als partijen die samen het stelsel gaan ontwikkelen en beheren en er op toezien dat de afspraken en standaarden worden gevolgd.

Met opmerkingen [Md23R22]: Dat zou heel mooi zijn maar is nu nog te vroeg om op te nemen als advies

gezamenlijke voorzieningen kunnen daarbinnen nog steeds bestaan, als dat de effectiviteit van het onderwijs ten goede komt.

Grote technologieplatformen positioneren zich steeds nadrukkelijker rondom digitale identiteiten en AI-gedreven dienstverlening. Hierdoor dreigt een situatie waarin publieke onderwijsprocessen afhankelijk worden van commerciële ecosystemen die primair worden gestuurd door marktbelangen in plaats van publieke waarden. Publieke regie is daarom geen bijzaak maar een randvoorwaarde: alleen wanneer onderwijsorganisaties gezamenlijk grip houden op identiteiten, verklaringen, standaarden en governance kan het onderwijs publieke waarden blijven beschermen in een steeds verder digitaliserende samenleving.

6.7. Transitie

Het bestaande stelsel van federatieve voorzieningen, wettelijk verankerde pseudoniemen en ketenkoppelingen is niet iets dat moet worden afgebroken – het is het vertrekpunt. De uitdaging is om stapsgewijs toe te werken naar het hierboven beschreven doelbeeld, zonder bestaande ketens te ontwrichten. Bestaande identiteiten worden niet abrupt vervangen, maar geleidelijk uitgebreid met onderwijsorganisatie-overstijgende identiteiten en verifieerbare verklaringen, waarbij interoperabiliteit tussen oud en nieuw de sleutel is.

Realiseerbaarheid is daarbij een expliciet uitgangspunt. De visie houdt rekening met de investeringspositie van dienstverleners, de bestuurlijke autonomie van onderwijsorganisaties – met name in het hoger onderwijs waar instellingen grotendeels zelf hun IAM-inrichting bepalen – en de wettelijke verankering van bestaande diensten en hun voorzieningen.

Self-sovereign identity (SSI) als technisch concept valt buiten de scope van deze visie. De visie beschrijft de gewenste regie van de onderwijsbetrokkene als principe; de technische implementatie daarvan – waaronder SSI en wallet-technologie – wordt uitgewerkt in het transitiepad. De wallet is een middel, geen doel op zich. Het toekomstige identiteitsstelsel is niet afhankelijk van één specifieke wallet-implementatie maar moet werken met elke wallet die aan de gestelde eisen voldoet.

Sommige stappen kunnen nu worden gezet – zoals de interoperabiliteit tussen ECK iD en eduID. Andere wachten op wetgeving, met name de aanpassing van de WHW en WEeB om persistente pseudonimisering in het hoger onderwijs mogelijk te maken. En een derde categorie wacht op Europese kaders, in het bijzonder de implementatie van de EUDIW. Hoofdstuk 7 werkt dit transitiepad verder uit.

7. Transitiepad

Volgt later.

8. Conclusie en vervolgstappen

Volgt later.