Verslag Edustandaard werkgroep Toegang

24 juni 2026

Aanleiding en doel

De kern van het besproken visiedocument is hoofdstuk 5, dat drie bouwstenen aandraagt voor een identiteitsvoorziening voor het gehele onderwijs. Het document wil niet alle bestaande sectorale rapporten herhalen, maar ze samenvoegen en er een sectoroverstijgende visie aan toevoegen – het metaforische 'nietje er doorheen slaan'. De context, begrippen en knelpunten zijn voor de leesbaarheid wel toegevoegd; daarvoor is een LLM gebruikt.

Een van de leidende ontwikkelingen is de wens voor meer autonomie: dat onderwijsinstellingen hun eigen keuzes kunnen maken over welke voorzieningen ze gebruiken, waar data is opgeslagen en wie de *kill switch* bezit. De visie stuurt aan op een voorziening in publiek beheer, maar wijst nog geen partij aan die dat moet oppakken. Buiten scope blijft ook hoe we daar precies komen.

De bal gaat hiermee terug van het kernteam naar de gehele werkgroep. Het kernteam vertegenwoordigt niet de gehele sector; er is inzet nodig van de werkgroep om het voorstel vanuit de achterban te toetsen, valideren en aan te vullen. Doel van de sessie: inzicht krijgen of dit voorstel sectorbreed gedragen kan worden, en zo ja, wat er daarvoor nodig is.

Introductie en eerste reacties

Het document schetst de huidige situatie: grote diversiteit aan identifiers, versnipperde provisioning, wens tot meer regie op gegevens en behoefte aan flexibiliteit. De drivers van de transitie zijn eIDAS 2.0, de Wet digitale overheid, het normenkader informatiebeveiliging en de flexibilisering van het onderwijs. De centrale vraag is hoe identity governance wordt ingericht – dat zal altijd een continuüm zijn tussen hub-gestuurd en point-to-point, waarbij het zwaartepunt kan verschuiven.

Vroeg in de discussie werd opgemerkt dat vertrouwen en betrouwbaarheid onvoldoende naar voren komen in de probleemstelling – die thematiek zit wel in de verklaringen, maar niet expliciet genoeg aan het begin. Ook werd de vraag gesteld: hoe komen we tot een levenslange identifier? Alles komt daar bovenop, maar zo'n identifier vraagt al veel inrichtingskeuzes. Het gesprek over de ontwerpprincipes bleek nodig; die waren tot dan toe te weinig het onderwerp van discussie geweest.

Discussie langs de ontwerpprincipes

De groep bracht het grootste deel van de sessie door met de acht ontwerpprincipes uit hoofdstuk 5. De uitkomst is conceptueel akkoord, met de aantekening dat een aantal principes in de tekst moet worden aangescherpt.

Principes 1–3: identiteit, contextspecificiteit en het gelaagd model

Vastgesteld werd dat een digitale identiteit geen authenticatiemiddel is – dat zijn twee wezenlijk verschillende dingen, en dit onderscheid moet explicieter in het document worden uitgewerkt. De ROSA maakt dit al helder; de visie moet dat overnemen.

Over het gelaagde identiteitsmodel (principes 2 en 3) ontstond de meeste inhoudelijke discussie, maar ook de meeste overeenstemming. Het model bestaat uit drie lagen:

1. *Foundational identity* – verankerd in het publieke domein (BRP/BSN voor Nederlanders, eIDAS voor EU-burgers). Expliciet aandachtspunt: ook voor niet-EU-studenten moet het model werken.
2. *Onderwijsidentiteit* – een sectoroverstijgende stamidentiteit die eenmalig wordt aangemaakt bij instroming in het onderwijs (eduID-achtig), afgeleid van de foundational identity via een onboardingsproces (bijv. via Studielink of NL Wallet). Publieke regie hoort hier te liggen.
3. *Contextspecifieke identiteiten/pseudoniemen* – per onderwijsorganisatie of keten, afgeleid van de onderwijsidentiteit.

De onderwijsidentiteit is dus een samenstel van de stamidentiteit en daarvan afgeleide pseudoniemen per context. Dit is een visie; de relatie tot concrete voorzieningen als ECK iD hoeft hier nog niet uitgewerkt te worden. Het model is ook geen Big Bang: sectoren zullen op verschillende momenten stappen zetten.

Principe 4: betrouwbaarheidsniveaus

Er moet een minimumniveau van betrouwbaarheid worden afgesproken voor wat in de keten rondgaat. eIDAS is het meest voor de hand liggende ordeningsmodel, maar bepaalde eisen op het laagste niveau zijn niet haalbaar of toepasbaar in het onderwijs. Bovendien gaat eIDAS alleen over authenticatie, niet over procesbetrouwbaarheid; het minimumniveau moet dus worden gerelateerd aan het specifieke proces en de bijbehorende risico's. OCW kan uitspraken doen over het beoogde niveau; een *race to the top* is niet het doel. Betrouwbaarheid begint overigens niet bij techniek, maar bij kwalitatief goede administraties, heldere rollen en contracten – credentials zijn de uitkomst van dat proces.

Principe 5: verifieerbare verklaringen

Steun voor het principe. Verifieerbare verklaringen maken het mogelijk om toegang te verlenen op basis van bewezen eigenschappen (diploma, inschrijving, niveau) zonder de volledige identiteit te onthullen. Het moet wel duidelijker worden welke gegevensuitwisseling op basis van wettelijke taak plaatsvindt, en wat onder regie van de deelnemer valt. Het bredere vraagstuk van gegevensuitwisseling en consent moet niet in deze visie worden meegenomen.

Principe 6: dataminimalisatie en doelbinding

Geen inhoudelijke bezwaren. De kern is flexibiliteit: per interactie bepalen welke attributen nodig zijn voor dat specifieke proces op dat moment, niet voor een hele instelling alles openzetten.

Principe 7: eigen regie

Eigen regie gaat hier primair over regie op de gegevens die vanuit het authenticatiemiddel beschikbaar worden gesteld – via verifieerbare verklaringen. Dat is wat anders dan self-sovereign identity in de volle betekenis (waarbij de lerende bij elke gegevensuitwisseling zelf aan de knoppen zit). SSI als model past hier niet, mede omdat er voor veel uitwisselingen gewoon een wettelijke basis bestaat. Het stelsel moet duidelijk maken waar een onderwijsbetrokkene wel en niet regie over kan voeren en waarom. Waar iemand dat niet zelf kan – jonge leerlingen, mensen met ondersteuningsbehoeften – moet vertegenwoordiging zijn geregeld: in sommige situaties kan en moet de school namens de leerling handelen. De wettelijke taak per sector (sterker in het funderend onderwijs dan in het ho) moet explicieter worden uitgeschreven.

Principe 8: publieke regie en leveranciersonafhankelijkheid

Breed gedragen. De scheiding tussen publieke identiteit en privaat authenticatiemiddel is precies de sleutel om publieke regie te behouden. Dit biedt ook een principiële grondslag voor discussies over partijen die nu de facto als identiteitsprovider fungeren zonder publieke governance. Het vertrouwensmodel moet expliciet zijn; impliciet vertrouwen op basis van bekendheid of netwerk is onvoldoende zodra het stelsel verder ontwikkelt.

De drie bouwstenen

Onderschreven we de drie bouwstenen, en is het federatieve vertrouwensmodel een doorontwikkeling van het huidige model – niet een vervanging? Dat werd bevestigd.

De **wallet** (bouwsteen 1/2) is een middel, geen doel. Het gevaar van de wallet als Big Bang moet worden vermeden. Van belang is ook dat identiteitsverklaringen en authenticatieverklaringen conceptueel worden onderscheiden.

Het **federatieve vertrouwensmodel** (bouwsteen 3) blijft het fundament voor governance, interoperabiliteit en wederzijds vertrouwen. De interoperabiliteit tussen ECK iD en eduID als eerste concrete scharnierpunt werd breed onderschreven.

Tekstuele aanpassingen nodig

Het document is open voor directe bewerkingen. Aan de leden die niet in het kernteam zitten, wordt gevraagd hun wijzigingen uiterlijk 3 juli door te voeren. De volgende punten vragen specifiek aandacht:

- Identiteit vs. authenticatiemiddel explicieter uitwerken
- Vertrouwen en betrouwbaarheid als zelfstandig thema toevoegen aan de probleemstelling
- Onderwijsdoelen als primaire driver toevoegen naast wetgevingsdruk
- Wettelijk mandaat per sector uitschrijven, inclusief de asymmetrie tussen fo en ho
- Eigen regie nuanceren: SSI expliciet buiten scope; vertegenwoordiging als mechanisme uitwerken
- Minimumbetrouwbaarheidsniveau benoemen, gerelateerd aan procesrisico's
- Wallet nadrukkelijk positioneren als middel
- Niet-EU-studenten adresseren in het identiteitsmodel

Vervolgstappen

De feedback wordt in drie stappen verwerkt:

- **Werkgroep** – reacties en aanpassingen direct in het werkdocument met track changes; t/m **vrijdag 3 juli**
- **Collega's** – check bij directe collega's; t/m **donderdag 3 september**
- **Bredere achterban** – bestuurlijke tafels en architectenraden; bij ons volgende overleg (9 september) bespreken we hoe we dit aanpakken.

Volgend overleg

Woensdag 9 september, 09:00–11:00, via Teams