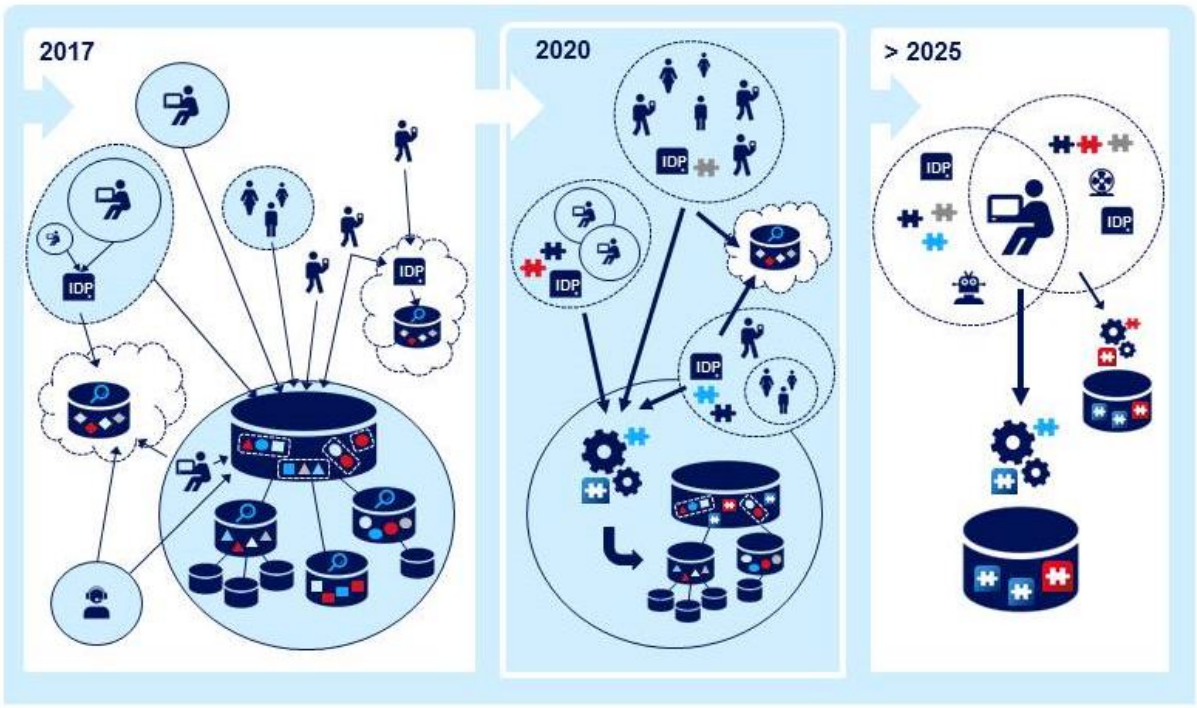
Op weg naar een IAA-stelsel Onderwijs



Werkgroep IAA-architectuur Onderwijs
Januari
Versie 0.91

Inhoudsopgave

1 Werken vanuit een visie

De ontwikkelingen rond digitalisering staan niet stil. Overheden en marktpartijen sturen er meer en meer op om hun diensten digitaal aan te bieden om hun diensten te verbeteren en tegelijkertijd kosten te besparen. Zo ontstaan er digitale gegevensverzamelingen die veel over ons als individu zeggen. En die gegevens zullen in toenemende mate bepalen hoe we worden bezien, behandeld en vertrouwd. De invloed van die digitale gegevens beperkt zich daarbij niet tot de digitale wereld en de digitale dienstverlening. Voorafgaand aan een bijeenkomst worden de sociale media als LinkedIn en Facebook gecheckt en worden bij het aanbieden van reclame wordt rekening gehouden met eerder klikgedrag en aankopen. En doet u een aankoop, dan zullen de mogelijkheden om te betalen afhangen van uw eerdere betaalgedrag. Smart watches gaan mogelijk weer een hele categorie gegevens toevoegen, zodat er nog meer digitaal beschikbaar komt dat ons beschrijft.
Onze digitale identiteit, of liever onze 'digitale doopceel' gaat dus een steeds belangrijkere rol spelen. Dit geldt uiteraard ook voor ons doen en laten in de digitale wereld. Grote data-aggregatoren zullen meer en meer gebruik maken van de informatie die individuen via hun diensten registreren. Hiermee zal men vaak vooraf met algemene gebruiksvoorwaarden moeten instemmen en is kan een vrijbrief zijn voor deze organisaties om de gegevens voor andere belangen te gebruiken dan het verstrekken van de dienst.

Het bieden van een gezond tegenwicht aan partijen die gegevensverzamelingen opbouwen en hier hun handel op kunnen bepalen, is derhalve een belangrijk maatschappelijk thema voor de komende jaren. Daarin is zeker ook een rol weggelegd voor de overheid. De consument vertoont wispelturig gedrag en is bereid zijn gegevens in ruil voor diensten of gewin vrij gemakkelijk weg te geven. Maar diezelfde consument heeft daarbij ook vaak het gevoel 'met de rug tegen de muur' te staan: het is een kwestie van de eenzijdige voorwaarden slikken of 'ernaast staan'. De individuele consument is in de onderhandeling over zijn gegevens dus zeer in het nadeel. Bovendien beziet dezelfde consument die gisteren wellicht zijn gegevens voor een klein gewin bewust heeft weggegeven, die deal morgen met andere ogen. Het zoeken naar de juiste middelen voor consumentenbescherming in deze is dus ingewikkeld.

We zien in Europees verband dat de bescherming van het privéleven en persoonsgegevens steeds belangrijker wordt. Naast bescherming van het privéleven, is in de grondrechten van de Europese Unie ook bescherming van persoonsgegevens een beschermd mensenrecht dat, ongeacht de context, altijd bescherming geniet. Met de komst van de nieuwe privacy-verordening wordt daaraan invulling gegeven. Deze Algemene Verordening Gegevensbescherming is op een aantal punten strenger dan de huidige wetgeving. Daarmee wordt ongelimiteerde gebruik van persoonsgegevens grotendeels aan banden gelegd.

De mix van instrumenten om privacy te beschermen, zal de volgende elementen kennen:

- Juridische bescherming tegen overmatige uitvraag en profilering. Door wet- en regelgeving en door gericht optreden van toezichthouders;
- Het maken van afspraken en opstellen van convenanten tussen betrokken partijen waarin de spelregels ten aanzien van identiteiten en gebruik van gegevens worden vastgelegd;
- Verhoogde bewustwording bij alle betrokkenen;

- Versterken van de onderhandelingspositie van de consument door belangenverenigingen en door het stimuleren van zelfregulering in bepaalde sectoren, bijvoorbeeld door het opstellen van gedragscodes etc.
- 'Empowerment' van de betrokken consument door:
    - Het verhogen van de transparantie: het handelen van partijen die consumentengegevens verzamelen meer inzichtelijk maken en zulks op een meer laagdrempelige manier;
    - Het vereenvoudigen en meer gebruikersgericht maken van het beheer van de 'instemmingen' van de consument en de mogelijkheid om in principe op elk moment een 'opt-in' of een 'opt-out' te kunnen doen.

Behalve de privacybescherming van de individuele gebruiker ten aanzien van her- en meergebruik van verstrekte gegevens aan al of niet direct gekozen dienstverleners, speelt ook de beveiliging van die gegevens een rol. Een dienstverlener kan zich prima aan de wet houden of aan de afspraken in een convenant, maar bij het gehackt worden van zijn dienst kunnen persoonsgegevens gekoppeld aan een bepaalde identiteit alsnog voor andere doeleinden "op straat" komen te liggen. Dat maakt dat vanuit privacywetgeving steeds meer invulling wordt gegeven aan de beveiligingsnormen die dienstverleners moeten aanhouden.

De bovengeschetste krachten en ontwikkelingen spelen ook in het onderwijs. We prijzen ons in deze gelukkig dat de sector die 'digitale educatieve content' levert zich bewust is van deze problematiek en daarom ook zelfregulering voorstaat. In dat verband worden er momenteel ook privacyconvenanten afgesloten in het kader van het Doorbraakproject ICT en Onderwijs.
Zoals bovengeschetst is een dergelijke zelfregulering echter slechts één van de instrumenten. De 'empowerment' van de onderwijsdeelnemer (c.q. zijn wettelijke vertegenwoordiger) is ook een instrument dat we niet moeten vergeten. Deze 'empowerment' vraagt ook om een architectuur die als referentie kan gaan dienen voor het richten van nieuwe ontwikkelingen en het geleidelijk en gefaseerd bijsturen van bestaande ontwikkelingen. Die toekomstvisie is in dit document uitgewerkt.

Aansluitend op deze visie wordt in dit document een concept voorgelegd over hoe identiteiten en persoonsgegevens ("attributen") van leerlingen en studenten dusdanig beheerd kunnen worden dat zij (of hun wettelijk vertegenwoordiger als ze jonger zijn dan 16 jaar) inzicht en controle hebben over het verstrekken van hun persoonsgegevens binnen het onderwijs. In het meest vergaande geval moeten ze in staat zijn per transactie te kunnen zien en bepalen of hun gegevens voor een bepaald doel beschikbaar wordt gesteld en wat hier mogelijk tegenover staat. Maar omdat dit niet altijd wenselijk of werkbaar zal zijn, kan worden gebruik gemaakt van constructies waarbij dit recht gemandateerd kan worden aan een andere partij (veelal de school). Voor het onderwijs is wettelijk vastgelegd dat de school in die rol mag opereren om goed onderwijs te garanderen. Dit vraagt wel extra zorgvuldigheid van de scholen omdat zij voor die leerlingen en studenten beslissingen nemen over de persoonsgegevens. Een school moet daarom wel kunnen verantwoorden welk gebruik er is gemaakt van de persoonsgegevens van leerlingen, en welke waarborgen de school heeft bedongen om de privacy van de leerlingen en studenten te kunnen garanderen. Het uiteindelijke doel moet een werkbaar IAA-stelsel zijn waarin "by design" een betere privacybescherming

van de onderwijsvolger gerealiseerd is onder andere door een gebruikersvriendelijk inzagerecht en een betere onderhandelingspositie ten aanzien attribuutverstrekking.

2 Ontwikkelingen

In dit hoofdstuk schetsen we eerst de algemene trends. Vervolgens komen we toe aan de specifieke trends in de onderwijswereld.

2.1 Ontwikkelingen in de samenleving

2.1.1 Digitale dienstverlening

De digitalisering van diensten neemt toe, zowel in het bedrijfsleven als bij de overheid. Met het programma Digitaal 2017 wil de overheid een versnelling creëren om burgers en bedrijven in staat stellen hun zaken met de overheid digitaal te kunnen regelen. Digitalisering is daarbij niet het uiteindelijke doel, maar een belangrijk middel om betere dienstverlening aan burgers en bedrijven te kunnen leveren. Hierbij wordt het belang onderkend om de klant centraal te stellen. Alleen met aandacht voor kwaliteit en direct contact tussen burgers, bedrijven en de overheid kan de digitalisering gerealiseerd worden in samenhang met verbetering van de dienstverlening en met een hogere kostenefficiëntie.

2.1.2 Internet of Things (IoT)

Met het Internet of Things (IoT) gaat het belang van betrouwbare digitale identiteiten toenemen. Hiermee komen de fysieke en digitale wereld dichter bij elkaar. Omdat dit niet beperkt blijft tot alleen fysieke dingen, heeft men het dan ook wel over het internet of Everything (IoE). Met IoT zullen verschillende apparaten ("devices") een eigen digitale identiteit hebben en kunnen ook onderling communiceren. Zij zullen aan een bepaald individu toebehoren welke andere rechten op het device heeft dan eventuele andere gebruikers van het device. Eigenaren kunnen zo configuraties instellen voor de verschillende gebruikers van de devices. Een voorbeeld uit de onderwijscontext: voor een visueel gehandicapte onderwijsvolger kan de lettergrootte op het te gebruiken onderwijsdevice automatisch vergroot worden op basis van de digitale identiteit (kenmerken). Deze heeft dan niet meer de hulp van een docent hiervoor nodig. Hierdoor kan de onderwijsvolger meer onafhankelijk handelen.
Devices kunnen in allerlei scenario's op basis van configuraties door de eigenaar van het device verschillend gedrag vertonen bij gebruik door verschillende digitale identiteiten (individuen). Omdat de devices ook online herkenbaar zijn kan dit gedrag ook op afstand geregeld worden. Het spreekt voor zich dat betrouwbaarheid rond digitale identiteiten en de beveiliging hierbij meer en meer een belangrijke rol gaan spelen.
Het gebruik van de devices creëert ook data over dat gebruik. Data die gekoppeld is aan een individu. Denk bijvoorbeeld aan een smart watch die zaken als hartslag registreert. Het vastleggen van die data en het mogelijk gebruiken van die data bij het leveren van bepaalde diensten is een ontwikkeling die sterk in opkomst is en die vragen stelt hoe hier mee om te gaan.

2.1.3 Het individu centraal creëert nieuwe business modellen

Het individu en hiermee zijn digitale identiteit komt steeds meer centraal te staan in de digitale wereld. Ook vanuit wetgeving wordt de positie van het individu versterkt. Het individu is niet langer passief, maar acteert zelf en individuen verenigen hun krachten in de digitale wereld. Crowdsourcing, crowdfunding en nieuwe disruptieve businessmodellen als Uber en Airbnb zijn voorbeelden waarbij effectief gebruik wordt gemaakt van de mogelijkheden die het contact met digitale identiteiten in zich heeft. Het maakt het voor meer traditionele, gevestigde partijen moeilijk om hiermee te

concurreren. Zij zien in toenemende mate het belang om het individu in de digitale wereld goed te kennen.
Er is een verschuiving van de huidige organisatie-centrische manier van handelen naar een manier van handelen waar de het individu centraal staat. Het individu is hierbij dus niet meer alleen een consument, maar levert zelf ook diensten waarbij de betrouwbaarheid wordt bepaald door de footprint in de digitale wereld.

2.1.4 Toenemend (economisch) belang van persoonsgegevens

Naast het individu worden ook de persoonsgegevens van dit individu steeds belangrijker. Vele partijen houden zich bezig met het aggregeren van allerlei persoonsgegevens en in sommige gevallen heeft men nog niet scherp wat met deze gegevens gedaan moet worden (zie het eerdere voorbeeld van de data die devices kunnen genereren). Men neigt naar het aggregeren van data om deze vervolgens te gebruiken voor allerlei analyses, bijvoorbeeld om het product te optimaliseren. Er is een sociale, economische en praktische waarde rond persoonsgegevens. Dit neemt in de toekomst naar verwachting alleen maar toe. Het mag duidelijk zijn dat hierbij het individu geen kennis heeft welke persoonsgegevens er gebruikt worden met welk doel. Partijen die persoonsgegevens willen verwerken doen er goed aan om de instemming voor het gebruik van deze gegevens goed te regelen. Ook hieruit ontstaat de noodzaak om het individu te kennen en te kunnen bereiken om de instemming te regelen. Om het individu te kennen zijn betrouwbare digitale identiteiten noodzakelijk. Hiermee worden dan ook deze digitale identiteiten net zo belangrijk als de data zelf.

2.1.5 Scherper toezicht en strengere wetgeving

Als gevolg van een toenemend aantal privacy-incidenten, en onthullingen over massale schending van de privacy van burgers zoals Snowden dat bekend maakte, leidt er toe dat er scherper wordt toegezien op de bescherming van privacy van burgers. Het afluisteren van regeringsleiders door bevriende staten, leidt tot grote verontwaardiging en politieke incidenten.

Mede door de toegenomen technologische ontwikkelingen mogelijkheden, heeft de Europese Commissie in 2012 besloten te komen tot een nieuwe privacy-wetgeving die voor alle landen in de Europese Unie gelijk is. Deze nieuwe Europese privacyverordening bevat een verbetering van de rechten van burgers door zijn onder meer: de rechten van betrokkenen te versterken waaronder het recht op dataportabiliteit, versteviging van de onafhankelijkheid en bevoegdheden van de nationale privacyautoriteiten, versterking van de verantwoordelijkheden van organisaties die persoonsgegevens verzamelen en gebruiken waaronder de invoering van de verplichting voor organisaties om datalekken direct te melden, introductie van een 'one stop shop'-systeem van toezicht voor bedrijven met vestigingen in meerdere EU-lidstaten of die diensten en goederen aanbieden in meerdere lidstaten waardoor bedrijven nog maar met één toezichthouder zaken hoeven te doen.

Verder wordt het verschil steeds zichtbaarder met landen buiten de Europese Unie: daar waar privacy bijvoorbeeld in Amerika gezien wordt als een consumentenrecht (waar een consument van mag afzien), wordt privacy in Europa gezien als fundamenteel mensenrecht dat onontvreemdbaar is.

2.1.6 Vertrouwen tussen individuen, diensten en stelsels

Peer-to-peer diensten versus de huidige situatie. <nog uit te werken>

2.2 Ontwikkelingen in het onderwijs

In een recent verschenen kaartenboek[1] opgesteld door Kennisnet en de Argumentenfabriek in samenwerking met bestuurders en informatiemanagers uit het po, vo en mbo staat het omgaan met data in het onderwijs centraal waarbij gekeken wordt naar verantwoordelijkheid van de school hierbij en naar de positie van de onderwijsvolger. Aanleiding voor dit onderzoek zijn de volgende trends:

- Verschuiving van focus: scholen hoeven zich met de komst van cloud computing minder druk te maken om de technische randvoorwaarden (want dat regelt de dienstverlener) maar moeten zich focussen op de verantwoorde omgang van de data van haar leerlingen en medewerkers.
- Meer verzamelde data: adaptief leermateriaal en persoonlijke leeromgevingen leiden tot meer persoonsgebonden gegevens die niet alleen binnen de muren van een school worden gebruikt en opgeslagen.
- Vaker inzicht in prestaties: de omgeving van de school eist steeds gedetailleerder inzicht in prestaties en het rendement van onderwijs. Zowel de overheid, de maatschappij als ouders van individuele leerlingen willen inzicht in de effectiviteit van de school, met gedetailleerde informatie over het verloop van processen en bereikte prestaties. We zijn met elkaar gewend geraakt aan de mogelijkheid alles wat we doen te kunnen 'tracken & tracen' en ook het onderwijs zal hier steeds meer mee te maken krijgen.

Naast deze trends zijn er nog enkele andere ontwikkelingen in het onderwijs zowel voor onderwijsvolgers als onderwijspersoneel die mede bepalend zijn voor de wijze waarop een IAA-stelsel en –diensten kan/kunnen worden ingericht.

2.2.1 Gepersonaliseerd leren

De klassen worden steeds groter en hiermee neemt de diversiteit in de klas toe. Voor docenten wordt het een steeds grotere uitdaging om iedere onderwijsvolger onderwijs te geven dat past bij zijn individuele mogelijkheden. Doordat ook in het onderwijs over het algemeen het aantal digitale diensten toeneemt, ligt er een kans om deze uitdaging in de digitale wereld op te vangen. Met een betrouwbare digitale identiteit van de onderwijsvolger kan er gepersonaliseerd leren geboden worden. Door gestructureerd digitaal leermateriaal aan te bieden dat gekoppeld is aan een leerlingvolgsysteem, een planningsprogramma en een digitaal portfolio, kan er met beperkte tijd en moeite van de docent een op het individu toegespitst onderwijs aangeboden worden. Deze ontwikkeling zal zich in de toekomst waarschijnlijk doorzetten. De diensten die hierbij gebruikt worden zullen op basis van de digitale identiteit van de onderwijsvolger en eventueel aanvullende gegevens moeten kunnen vaststellen dat het hetzelfde individu betreft.

Naast eenduidigheid rond de identiteit van het individu geeft dit ook aan dat het delen van persoonsgegevens zal toenemen. Hierbij is het belangrijk dat de onderwijsvolger en eventuele vertegenwoordigers inzicht wordt geboden welke gegevens er waar gebruikt worden om deze vorm van gepersonaliseerd leren te realiseren.

[1] *Omgaan met data in het onderwijs, van en voor bestuurders in het po, vo en mbo*, november 2015

In het laatste hoofdstuk van hierboven genoemde publicatie[2] worden twee opties verkend in zake het toestemming geven voor gebruik van persoonsgegevens: een organisatiegerichte en een gebruikersgerichte benadering. De terechte kanttekening hierbij is dat het organiseren van expliciete toestemming van de gebruiker (onderwijsvolger) alleen nodig is voor gegevens die niet strikt noodzakelijk zijn voor het geven van onderwijs of het begeleiden van leerlingen. Want: gegevens die echt nodig zijn voor het onderwijsproces of begeleiden van leerlingen mogen scholen altijd gebruiken en uitwisselen. Dit is ook zo in de onderwijswetgeving vastgelegd. Niettemin blijft het daarbij van belang dat de school transparant is over welke gegevens er op welk moment nodig zijn en met welke partners zij dat doet om het onderwijs goed te organiseren.
Bovendien is de algehele verwachting dat naarmate maatwerk aan individuele leerlingen via inzet van ICT toeneemt en scholen dus meer kunnen doen buiten het 'strikt noodzakelijke onderwijs', het in de toekomst steeds vaker nodig zal zijn om andere toestemmingsmodellen te organiseren.

Daarnaast zal het belangrijk zijn dat de onderwijsvolger en eventuele vertegenwoordigers kunnen beschikken over de betreffende gegevens in de mogelijk verschillende systemen en dat er bij het overstappen naar een andere onderwijsinstelling deze gegevens probleemloos meegenomen kunnen worden indien gewenst.

2.2.2 Een leven lang leren

Het "leven lang leren" is een belangrijk streefbeeld binnen het onderwijs. Niet alleen tijdens de reguliere onderwijscarrière zal de onderwijsvolger gegevens willen vasthouden en hergebruiken. Ook uitgeschreven onderwijsvolgers willen na hun "onderwijsleven" nog kunnen doorleren. Vaak zal een medewerker nog een cursus willen volgen om zich bij te scholen of aan een vervolgopleiding willen beginnen. Naast dat het gangbaar is dat het opleidingsinstituut dan bepaalde persoonsgegevens zal willen registreren zal deze meer en meer ook inzage willen hebben in bepaalde onderwijskundige gegevens. Dit geldt overigens ook voor potentiële nieuwe werkgevers.

Ontwikkelingen rond het "leven lang leren" geven aan dat er eenduidigheid rond de identiteit van het individu noodzakelijk is en dat dit thema zal bijdragen aan het toenemen van het verstrekken van persoonsgegevens. Hoever men mag gaan, moet het onderwerp zijn van nader te ontwikkelen beleid. Het gaat daarbij overigens niet alleen over continuïteit, nl. het hergebruik van eerder opgegeven of gegenereerde gegevens, maar ook om discontinuïteit, het recht om bepaalde gegevens te kunnen vergeten.
Het is derhalve ook belangrijk dat de onderwijsvolger zelf daarin kan kiezen welke gegevens hij wel en welke gegevens hij niet over wenst te (laten) dragen en dat hem inzage geboden wordt in deze verstrekkingen.

2.2.3 Toenemende regeldruk

Een belangrijk thema in het onderwijs is het terugdringen van de lastendruk. Dat lijkt op gespannen te staan met strenger wordende privacywetgeving. Hoewel onderwijsinstellingen reeds verantwoordelijk waren voor het aanleggen en beschermen van de gegeven van hun leerlingen, zien zij nu ook in dat zij daar meer voor moeten

[2] *Omgaan met data in het onderwijs, van en voor bestuurders in het po, vo en mbo*, november 2015, pag. 23 e.v.

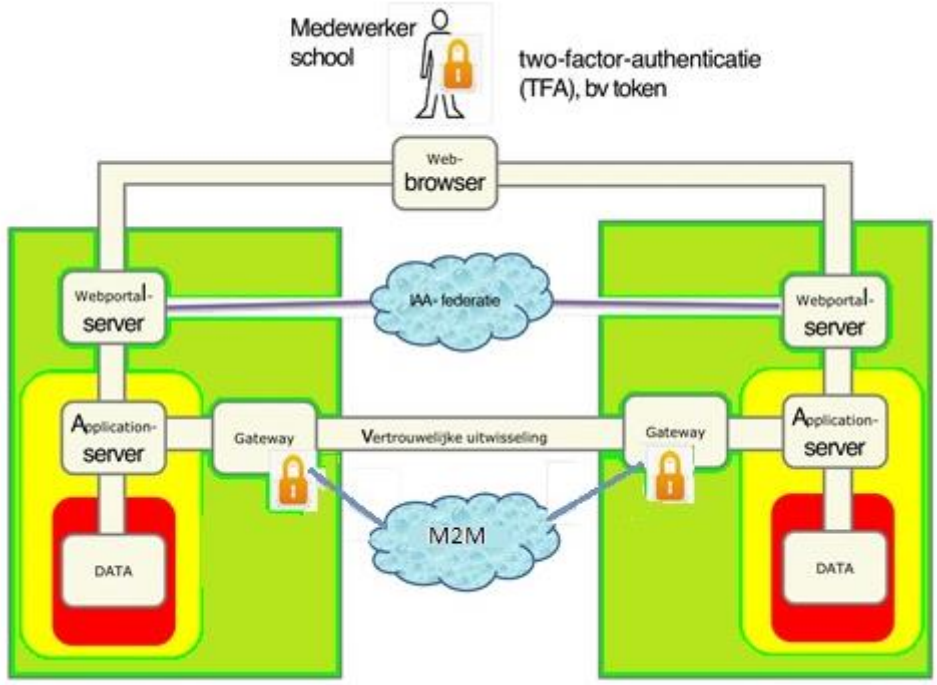
doen. Door de toegenomen aandacht is te verwachten dat meer onderwijsvolgers gebruik zullen maken van hun inzagerecht (art. 35 WBP): welke gegevens heeft de school van mij verzameld en aan wie worden die verstrekt?
Ook zullen scholen hun gegevensleveringen aan uitgevers en distributeurs meer 'op maat' moeten maken en hier ook beter verantwoording over gaan afleggen. Een belangrijke stap hiertoe is gemaakt met de privacyconvenanten in het PO en VO waarbij ook privacybijsluiters zijn voorzien die leveranciers bij hun diensten moeten leveren en die de school beschikbaar kan stellen aan onderwijsvolgers en hun wettige vertegenwoordigers.

2.2.4 Internationalisering onderwijs

De "consumptie" van onderwijs blijkt niet langer gebonden te zijn aan streek, land of werelddeel. Steeds vaker sprokkelen studenten met name in het HO maar deels ook al in het MBO hun curriculum bijeen door het volgen van modules op verschillende onderwijsinstellingen. En die bevinden zich over de gehele wereld. Internet biedt bovendien de mogelijk om studies over de gehele wereld in het land van herkomst van de student te volgen: achter de computer in de eigen huiskamer.
Dit is ook van invloed op de IAA-voorzieningen. Het maakt het zeer wenselijk dat aangesloten wordt bij internationaal erkende standaarden en stelsels van identiteiten. Een IAA-stelsel kan dan een 'poort naar de internationale onderwijswereld' zijn, waarbij identiteiten worden verstrekt aan populaire buitenlandse aanbieders van digitale content, maar waarbij de privacy van de onderwijsvolgers zo goed mogelijk wordt beschermd. Daarnaast is een dergelijke 'poort' benadering ook zinvol voor het terugkoppelen van leeractiviteiten en –resultaten.

2.2.5 Vertrouwensniveau onderwijspersoneel

De school is eindverantwoordelijk voor privacy en beveiliging van de leerlinggegevens. Dit is bevestigd in de 'kamerbrief over privacy en informatiebeveiliging' (3 juli 2015). Onderwijsmedewerkers handelen namens de school in tal van processen waar uitwisseling van leerlinggegevens en andere vertrouwelijke gegevens aan de orde is. Dat kan via zogeheten portalen (human-to-machine, H2M) maar ook door opdracht te geven om een pakketje gegevens als digitaal bericht van het eigen schoolsysteem naar het systeem van een andere ketenpartner te sturen (machine-to-machine, M2M).
Gegeven de eindverantwoordelijkheid van scholen is het voor uitwisselingen van gegevens waarbij meer dan normaal vertrouwen is vereist, niet alleen zaak om de verbindingen goed te beveiligen zodat onbevoegden niet achter de gegevens kunnen komen.
Het goed kunnen identificeren van een onderwijsmedewerker door een systeem is dan ook noodzakelijk voor het borgen van de privacy en is een combinatie van meerdere maatregelen. De levenscyclus van de identiteit van een onderwijsmedewerker volgt meerdere stappen waarin die maatregelen toegepast dienen te zijn. Ten eerste moet de identiteit van de persoon geverifieerd worden bij het aanmaken van een account. Ten tweede moeten er maatregelen getroffen worden om de gebruiker goed te authenticeren in een systeem bij het inloggen. Op dit moment wordt er vaak gebruik gemaakt van slechts username/wachtwoord, maar op basis van bestaande richtlijnen en best practices lijkt aanvullende identificatie (two-factor-identificatie, 2FA), bijvoorbeeld via een token, noodzakelijk. Tot slot moet het intrekken van toegang ook goed geregeld zijn, immers een persoon houdt niet voor eeuwig toegang.



2.2.6 Onderwijspersoneel werkt voor meerdere instellingen

In het hoger onderwijs is het al sinds mensenheugenis gewoon dat medewerkers voor meerdere instellingen werkzaam zijn. Verder kunnen medewerkers namens hun instellingen participeren in onderzoeken waarbij meerdere instellingen zijn aangehaakt. Maar ook in de andere sectoren is dit verschijnsel zeker niet onbekend. In het po bijvoorbeeld kan een oproepkracht voor meerdere scholen werken.
De beheerders van de registratiesystemen die de medewerkers gebruiken voor de uitoefening van hun werk hebben de identificatie en authenticatie vaak op eigen manier ingericht en dat verschilt onderling. De medewerker wordt zodanig geconfronteerd met extra overhead. Bovendien wordt de toegang tot het gebruik van bepaalde hulpmiddelen over verschillende instellingen heen (eigen licenties bijvoorbeeld) bemoeilijkt.
Hoewel de rollen en de bevoegdheden kunnen wisselen per gebruikssituatie is het aannemelijk dat de identificatie en de authenticatie voor heel veel gevallen op een identiek niveau kan worden uitgevoerd.

2.3 Wet- en regelgeving

Europa heeft een lange geschiedenis, zowel waar het gaat om de bescherming van de privacy van het individu, als op het gebied van elektronische identificatie en handtekeningen.
De laatste ontwikkelingen zijn twee Europese verordeningen voor die gebieden:

- De eIDAS verordening, die het grensoverschrijdend gebruik van elektronische identiteiten en vertrouwensdiensten regelt in Europa. Deze gaat wezenlijk verder en komt in de plaats van de Richtlijn Elektronische Handtekeningen;
- De Europese Algemene Verordening Privacybescherming, die in de plaats komt van de eerdere Europese Dataprotectierichtlijn en nationale privacywetgeving.

2.3.1 eIDAS Verordening

Op 23 juli 2014 is de Europese Verordening betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt (eIDAS[3] verordening) aangenomen. eIDAS is gericht op het verwijderen van bestaande belemmeringen voor de digitale ontwikkeling in Europa door het verstrekken van de juridische basis voor een wederzijdse erkenning van elektronische identificatie en authenticatie.

Met de eIDAS-regulering wordt nagestreefd dat:

- Personen en bedrijven hun eigen nationale elektronische identificatie regelingen (eID middelen of stelsel) kunnen gebruiken om toegang te krijgen tot openbare diensten in andere EU- landen (waar eID's kunnen worden gebruikt voor toegang tot elektronische dienstverlening). De voorwaarde is wel dat dergelijke nationale eID Stelsels (zoals Idensys) worden genotificeerd;
- Er een Europese interne markt voor elektronische vertrouwensdiensten ontstaat, voor elektronische handtekeningen, elektronische zegels, tijdstempel, elektronische delivery service en de website authenticatie. Om dit te realiseren wordt ervoor gezorgd dat de vertrouwensdiensten (ook technisch) over de grenzen heen werken en geaccepteerd worden. Elektronische handtekeningen krijgen daarbij dezelfde juridische status hebben als de traditionele handgeschreven handtekening en elektronische diensten Het borgen van de rechtsgeldigheid van deze diensten zal ondernemingen en burgers zekerheid en het vertrouwen geven om van (internationale) digitale diensten gebruik te maken wat de nodige kostenbesparing oplevert.

In Nederland zouden de authenticatiediensten van PKIoverheid, DigiD, eHerkenning en Idensys in beginsel in aanmerking komen voor notificatie, omdat het alle eID stelsels zijn zoals de eIDAS verordening bedoelt. Dergelijke elektronische identificatie alsmede vertrouwensdiensten als elektronische handtekeningen zouden direct nuttig bruikbaar zijn voor onderwijsprocessen. Denk bijvoorbeeld aan het digitale inschrijvingsproces, waarin authenticatie van de gebruiker en ondertekenen van documenten aan de orde zijn.

eIDAS reguleert ook de authenticatie van webdiensten, zij het dat er voor de inhoudelijke eisen nauw wordt aangesloten op de reeds bekende eisen van het CA Browser Forum, die al worden gehanteerd door de meeste browsers. Als vertrouwensdiensten vallen ze wel onder het toezicht door de beoogd toezichthouder in Nederland, de Autoriteit Telecom (AT). Dit raakt (zij het zijdelings) de vele websites binnen het onderwijs die beveiligd zijn met een certificaat.

Naar verwachting zal er ook in de toekomst gebruik gemaakt worden van elektronische eID en vertrouwensdiensten van de overheid. We hebben dus binnen het onderwijs op termijn direct te maken met de eIDAS. verordening.

Omdat onderwijs een vorm van publieke dienstverlening is en veel diensten inmiddels ook langs elektronische weg met behulp van een elektronische identiteit worden ontsloten, is er dus ook de verplichting om deze te ontsluiten voor genotificeerde eID's

[3] Europese Verordening eIDAS: http://ec.europa.eu/digital-agenda/en/trust-services-and-eid

uit andere lidstaten. Het is de planning dat Idensys hiervoor voorzieningen gaat bieden, zodat buitenlandse eID's ook binnen Idensys bruikbaar worden. Alleen om deze reden al is het nodig dat eID's die binnen Idensys zijn toegelaten, ook bruikbaar worden in de context van het onderwijs.

In dit verband is het gewenst om tenminste de basale authenticatie (eID) functie van Idensys ook in het IAA-stelsel te ontsluiten. Maar waarschijnlijk is het ook gewenst dat identificerende attributen vanuit Idensys en van genotificeerde buitenlandse eID's beschikbaar komen in het IAA-stelsel.

2.3.2 Privacyverordening

Rond privacywetgeving zal op Europees niveau binnenkort een belangrijke verandering plaatsvinden. De huidige Europese Richtlijn uit 1995 waar de Nederlandse Wet bescherming persoonsgegevens (WBP) op gebaseerd is zal vervangen worden door een nieuwe Europese privacyverordening (de General Data Protection Regulation (5853/12)). De Verordening is op het moment van inwerkingtreding aan te merken als een wetgevend instrument. Het staat de lidstaten niet vrij om, zoals dat wel het geval is bij een richtlijn, de bepalingen op eigen wijze te implementeren (zoals nu met WBP).

Doordat de tekst van verordening nu nog niet op alle punten vast staat, kan er ook nog niet met zekerheid uitspraken worden gedaan over de volledige impact. Wel is het beeld dat de verordening op een aantal punten strenger zal zijn, en zal leiden tot een eenvormiger privacybescherming binnen de Europese Unie. Het is wel zeer waarschijnlijk dat de volgende aspecten onderdeel worden van de Verordening:

- Bevat strengere regels met betrekking tot het verwerken van persoonsgegeven en geeft toezichthouders uitgebreidere sanctiebevoegdheden bij overtreding hiervan.
- Meldplicht voor datalekken.
- Eisen m.b.t. de bewerkersovereenkomst: duur van de gegevensverwerking, de specifieke doeleinden voor verwerking, het soort persoonsgegevens en een beschrijving van de betrokkenen.
- Publieke instanties zijn verplicht een functionaris gegevensbescherming aan te stellen.
- In bepaalde gevallen van gegevensverwerking dient de verantwoordelijke – voorafgaand aan de verwerking een 'data protection impact assessment' uit laten voeren.
- versteviging van de onafhankelijkheid en bevoegdheden van de nationale privacyautoriteiten;
- Er moet als uitgangspunt vooraf uitdrukkelijke toestemming gegeven zijn voor de verwerking van persoonsgegevens.
- Extra regels voor personen jonger dan 18 jaar.

3 Ontwikkelingen uitgewerkt in een visie

3.1 Omgaan met identiteiten in verschillende domeinen

Het voorgaande geeft aan dat de digitale wereld niet alleen meer en meer integreert met de fysieke wereld, maar doordat er steeds meer digitale diensten aangeboden worden zal het individu ook in de digitale wereld in een veelvoud van verschillende domeinen acteren, zoals dat nu al in de fysieke wereld gebeurd. Een vader die zelf studeert schrijft als vertegenwoordiger van zijn minderjarige dochter deze tevens in voor het primair onderwijs. Een student binnen het wetenschappelijk onderwijs is tevens werknemer van een onderwijsinstelling waar hij doceert. Deze domeinen worden in de digitale wereld bepaald door de dienst die wordt afgenomen. Een individu neemt zo een digitale dienst af bijvoorbeeld als burger, consument, patiënt of werknemer (zie Figuur 1).

Figuur 1 – Een individu acteert in de digitale wereld in een bepaalde context

Hoog over kan gesteld worden dat in elk domein bepaalde (eigen) identificerende gegevens nodig zijn. Vaak bepaalde identiteiten en een groepje attributen. Binnen het onderwijs wordt het PGN gebruikt als identiteit van een onderwijsvolger binnen formele administratieve processen maar zijn er voor de overige processen meerdere invullingen.

Zoomen we in op een domein, dan zullen we zien dat breed bruikbare identiteiten als het PGN minder gewenst zijn en dat fijnmaziger identiteiten bij voorkeur worden toegepast.

Een individu zal zichzelf willen bedienen van meerdere (pseudo-)identiteiten, die liefst uniek en persistent per dienst te gebruiken zijn. Dit om privacybescherming optimaal te waarborgen onder andere door de koppelbaarheid van gegevensattributen van een individu in te perken. Daar waar een bepaalde dienstaanbieder attributen van een andere dienst nodig heeft om richting een individu een eigen dienst te leveren worden die gegevens geleverd zonder dat daarbij beide dienstaanbieders een en dezelfde identiteit moeten hanteren. Dit vraagt om andere koppelmechanismen dan het verstrekken en hanteren van ketenidentiteit dan wel sectoridentiteit.

3.2 Authenticatie: van 'stovepipes' naar een generieke infrastructuur

Klassiek was authenticatie iets dat elke aanbieder van elektronische diensten in zijn eigen domein regelde. Met als gevolg een snel groter wordende 'digitale sleutelbos'. Uiteraard willen we dat niet, want het is voor de gebruiker niet te doen en bovendien is het uiteindelijk ook niet te betalen, zeker als hogere betrouwbaarheidsniveaus gewenst worden.

We groeien daarom toe naar breed bruikbare authenticatievoorzieningen. De laatste jaren kennen we zoiets als sectorbrede voorzieningen in Nederland: DigiD voor de overheid, een bankkaart voor de financiële diensten, de UZI-pas voor zorgverleners et cetera.

Nu staan we aan de vooravond om van die authenticatie een werkelijk generieke infrastructuur te maken in Nederland, met de invoering van Idensys. Idensys maakt authenticatiemiddelen ook bruikbaar in andere domeinen. Idensys biedt in concept ook de voorziening om daarbij de voor het domein van de aanbieder van de elektronische diensten relevante identiteiten te leveren, door die identiteiten in een koppelregister bij de houden. Vooralsnog is dat beperkt tot het leveren van een BSN voor die partijen die het BSN mogen ontvangen.

Eenzelfde benaderwijze (hergebruik authenticatiemiddelen) hanteren we ook in het IAA Stelsel voor het onderwijs. Sterker nog, de meeste zaken kunnen direct worden gekopieerd van Idensys.
Er is echter ook een aantal in het oog springende punten waarin het IAA-stelsel voor het onderwijs afwijkt van Idensys c.q. daar aanvullende diensten bovenop levert:

- Anders dan in Idensys, is er ruimte voor lagere betrouwbaarheidsniveaus en uitgifte door onderwijsinstellingen die onder een lichter toezichtsregime hiervoor staan;
- Anders dan in Idensys is er ruimte voor een variëteit aan verschillende pseudoniemen, die in een nummervoorziening worden gemaakt en/of worden beheerd. In aanvulling op Idensys levert het IAA-stelsel onderwijs identiteiten voor aanbieders of ketens, nauwkeurig passend op de behoefte aan het dienstverlenende proces.
- In aanvulling op Idensys worden voor attributenverstrekking uitgebreider faciliteiten geboden, waarin de privacy van de eindgebruiker centraal staat en

waarin de eindgebruiker daarvoor wordt 'empowered'. In Idensys lijkt user consent vooral een 'afterthought' te zijn, waarna daarvoor enkele functies zijn toegevoegd aan reeds bestaande business rollen. Een zuivere 'separation of concerns' wordt hiermee echter niet bereikt;

3.3 Vertrouwen op een stelsel in plaats van zelf regelen

Voor veel partijen in het onderwijs zal het een 'quantum leap' zijn om authenticatiemiddelen niet meer zelf uit te geven, maar om te vertrouwen op de authenticatie die elders, in het IAA-stelsel wordt uitgevoerd. Zo zal dat ook gelden voor de levering van attributen. Het bouwen aan het vertrouwen tussen de verschillende partijen zal nodig zijn om inderdaad te vertrouwen op de gegevens van een andere partij.

3.4 Verstrekken van persoonsgegevens

3.4.1 Huidige situatie

Individuen worden idealiter bij afname van diensten herkend op basis van een (specifiek) pseudoniem (identiteit). Zij zouden hierbij het vermogen moeten hebben om geïnformeerde keuzes te maken over het wel of niet verstrekken van bepaalde aanvullende gegevens. Hiermee heeft de persoon zelf inzicht in de verstrekte gegevens aan de betreffende dienst en heeft zelf de controle om verstrekte data te minimaliseren. Deze verstrekte gegevens kunnen noodzakelijk zijn om zichzelf online herkend te laten worden, of om over bepaalde aanvullende bevoegdheden te kunnen beschikken (bijvoorbeeld op basis van het gegeven of het individu ouder dan 18 jaar is). De diensten en partijen die over dergelijke gegevens willen of moeten beschikken hebben er belang bij dat het individu vertrouwen in de dienst heeft, de omgeving is veilig en er wordt conform afspraken gehandeld.

In authenticatiestelsels zoals de Kennisnetfederaties en SURFconext, maar ook in stelsels als eHerkenning en Idensys heeft de levering van attributen/ gegevens wel de aandacht, maar is de visie nogal beperkt als het gaat om de regie over zijn gegevens bij de burger zelf te leggen. Momenteel is het feitelijk beperkt tot het meeleveren door een authenticatiedienst van enkele aanvullende attributen. In het algemeen gaat het daarbij om attributen waar de authenticatiedienst / middelenuitgever kan beschikken vanuit het registratie- en uitgifteproces. De authenticatiedienst levert attributen desgevraagd na instemming van de gebruiker via de makelaar aan de dienstaanbieder.

Het mechanisme voor verstrekking van attributen verloopt in die bestaande situaties via hetzelfde mechanisme als waarmee de authenticatieverklaring geleverd wordt. We zien hierbij een aantal beperkingen:

1. In de huidige onderwijsketens worden de diensten niet altijd op een gewenst detailniveau geregistreerd. De authenticatieverklaring kan dan attributen leveren aan een dienst die deze gegevens niet nodig heeft en is in strijd met de principes van doelbinding en dataminimalisatie.
2. Als een gebruiker meerdere authenticatiediensten gebruikt voor verschillende dienstaanbieders zal de gebruiker bij elke authenticatiedienst de attributen en autorisaties moeten registreren en bijhouden.
3. De attributen die geleverd worden zijn beperkt tot de set die de gebruiker bij de authenticatiedienst registreert. Zoals aangegeven bij de ontwikkelingen in de

samenleving en het onderwijs zullen er meer en meer persoonsgegevens uitgewisseld moeten worden, ook aan diensten waar het individu niet zelf direct mee interacteert.

3.4.2 Gewenste situatie

De dienstaanbieders zijn verantwoordelijk voor bepaalde processen en kunnen hiermee niet uitsluitend als afnemer maar juist ook als bron gezien worden van bepaalde persoonsgegevens. Met het "halen bij de bron"-principe ontstaat er een complex landschap waarin vele persoonsgegevens geregistreerd en verstrekt kunnen worden.

De huidige stelsels bieden geen mechanismen om verstrekkingen uit willekeurige bronnen anders dan de authenticatiediensten te autoriseren. Ook zijn er geen mechanismen om inzage te krijgen wanneer deze gegevens uitgewisseld worden. Daarnaast speelt ook nog dat met het handhaven van het eenmalig verstrekken en meervoudig gebruik bronnen met betrekking tot bepaalde persoonsgegevens een bepaalde status hebben (zoals een authentieke bron of lokale afgeleide registratie).

In lijn met de visie die elders binnen de overheid ook wordt nagestreefd[4] ambiëren we een stelsel waarin het individu en zijn privacy centraal staan. Daarbij willen we ons niet beperken tot het strikt wettelijk verplichte, maar willen we het individu een instrument in handen geven, waarmee hij zelf de regie over de verstrekte gegevens wordt geboden. Het IAA-stelsel bevat daartoe een dienst waarmee het individu één plek krijgt waar de autorisaties voor verstrekking geregistreerd kunnen worden en waar de momenten van verstrekking en andere details inzichtelijk gemaakt worden. De dienst die hiervoor verantwoordelijk is, noemen we de Inzage- & Instemmingsdienst (I&I-dienst). Deze dienst biedt het individu voldoende informatie zodat deze een geïnformeerde beslissing kan maken over het wel of niet verstrekken van bepaalde gegevens. Er wordt dus ook aangegeven wat de consequenties zijn van het niet verstrekken van een bepaald gegeven. Ook in geval er geen sprake is van toestemming, geeft deze dienst tenminste inzage wat er met de persoonsgegevens is gedaan.

De Inzage- & Instemmingsdienst heeft een duidelijke rol in *Resource & Access management*, maar neemt geen deel in de gegevensuitwisseling. Het is dus geen centrale attributenopslag waaruit attributen geleverd worden. Een geautoriseerde afnemer van persoonsgegevens kan deze bij de betreffende bron ophalen. Er moet dus geregeld worden dat afnemers de locaties van de bronnen kunnen bepalen (of vice versa).

Met een dergelijke gecontroleerde verstrekking van gegevens komt ook de roep voor een eigen digitale ruimte of 'kluisje' snel om de hoek kijken. Hoewel het gebruik van de verschillende (authentieke) bronnen de voorkeur heeft, wordt ook onderkend dat deze niet altijd gebruikt kunnen worden voor het doel dat het individu voor ogen heeft. Deze bronnen ontstaan doordat partijen die gegevens verwerken voor specifieke processen.

---

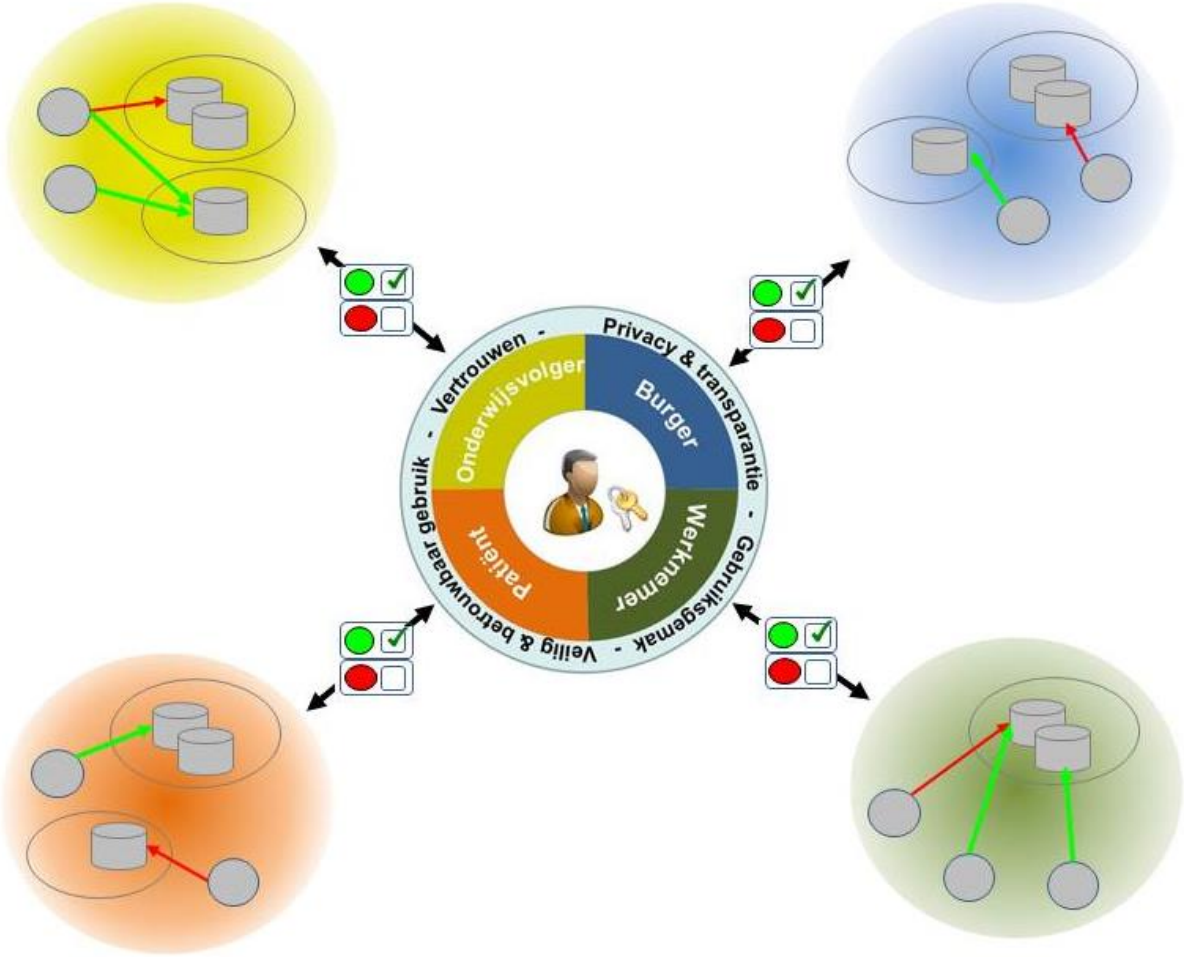
[4] Zie bijvoorbeeld het project "Regie op gegevens", waarin kennis en ervaringen in zake de ontwikkelingen op het gebied van "digitale kluisjes" en andere privacybevorderende voorzieningen tussen diverse overheidssectoren worden gedeeld, en het in opdracht van het Ministerie van BZK opgestelde adviesdocument *Eigen gegevens, eigen regie?,* Schoenmakers, Sloots en Wendt, oktober 2014. Te downloaden op: https://www.rijksoverheid.nl/documenten/rapporten/2014/10/01/eigen-gegevens-eigen-regie

Dit doel maakt het niet zonder meer mogelijk voor het individu om deze gegevens te gebruiken en te combineren voor andere doelen of in andere contexten.
Daarnaast speelt ook de bewaartermijn een beperkende rol. Het individu wil mogelijk vele jaren lang over de betreffende gegevens kunnen beschikken, denk bijvoorbeeld hierbij aan het thema “leven lang leren”. De partijen die deze gegevens beheren dienen echter bepaalde gegevens na een bepaalde bewaartermijn te verwijderen. Dit gaat vóór het belang van het individu.

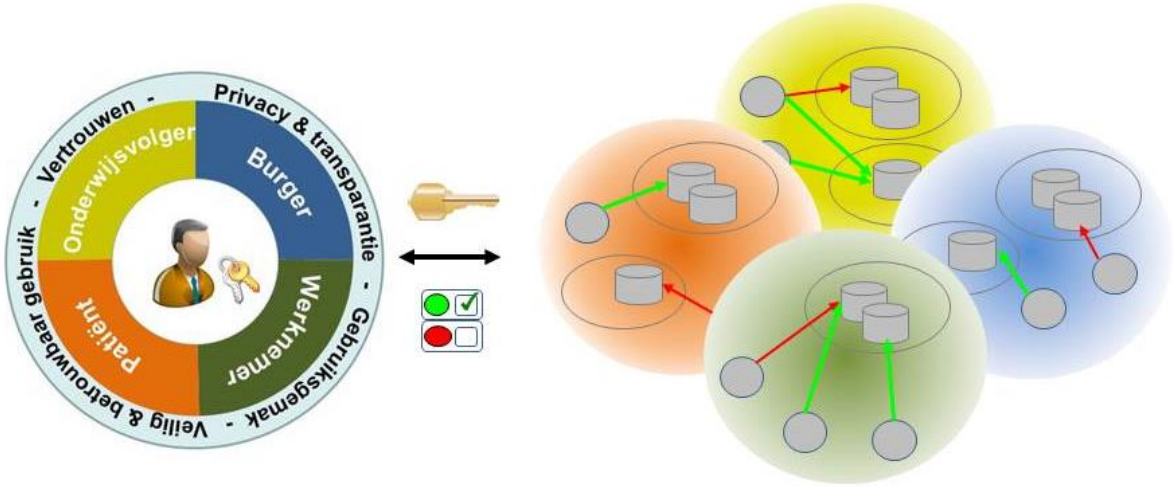
Een persoonlijke bron (“digitale kluis”) lijkt daarom wenselijk. Het individu moet dan wel probleemloos data van de verschillende (authentieke) bronnen naar deze persoonlijke bron kunnen halen. De data in deze bron kan het individu vervolgens naar eigen inzicht tegen zelf te bepalen voorwaarden verstrekken. Eventueel is bijvoorbeeld ook anonieme verstrekking mogelijk, wat nuttig kan zijn voor bepaalde analyses of onderzoeken.

Er is een vertrouwde derde partij, een stelselautoriteit, nodig die op de naleving van afspraken toeziet. Dit zijn deels functies in het beveiligings- en assurancedomein, maar deze heeft ook een taak om de positie van het individu te ondersteunen. De stelselautoriteit moet er voor zorgen dat het individu daadwerkelijk naar eigen inzicht zijn gegevens kan verstrekken onder voorwaarden die door de stelselautoriteit ondersteund worden en geborgd zijn.

Het organiseren van een attributenketen op basis van dit mechanisme is complex en zal tijd vragen. Daarnaast is de onderwijssector niet het enige domein waar dit zal gaan spelen. Zoals eerder aangegeven handelt een individu in verschillende domeinen. Naar verwachting zullen er binnen deze verschillende domeinen, zoals de centrale overheid en zorg ook dergelijke diensten ter beschikking gesteld gaan worden. Zo heeft het individu in de verschillende contexten nog steeds te maken met verschillende I&I-diensten (zie Figuur 2). Ook dit is dus nog niet een optimaal scenario, maar wel een belangrijke stap naar volledige integratie over alle domeinen van interoperabele attributenketens en identiteitsmanagement (zie Figuur 3).



Figuur 2 –De instemming en inzage dienst is per context centraal geregeld.



Figuur 3 – Onderliggende mechanismen zijn over alle contexten gestandaardiseerd

4 Afkortingen / Verklarende woordenlijst

De begrippen en omschrijvingen zijn deels van het Afsprakenstelsel Elektronische Toegangsdiensten (AET)[5] overgenomen. Het afsprakenstelsel is een set van technische, functionele, juridische en organisatorische afspraken op basis waarvan eHerkenning en Idensys worden geleverd. De afspraken hebben als doel om samenwerking en zekerheid in het Netwerk te garanderen.

In de lijst hieronder zijn voor het gemak een aantal begrippen overgenomen en er zijn een aantal aanvullende begrippen opgenomen die specifiek voor dit document zijn.

Begrip	Omschrijving	Bron
Afsprakenstelsel	Het geheel aan afspraken op gebied van organisatie, besturing, toezicht, beheer, architectuur, toepassingen, techniek. Procedures en regels aangaande het Netwerk (voor Elektronische Toegangsdiensten) in een bepaalde vastgestelde versie. Het doel is betrouwbare authenticatie en verstrekking van identiteitsinformatie op basis van de eHerkenningsdiensten van een goed gereguleerd netwerk voor eHerkenning.	AET
Applicatie attribuut	Dit is een attribuut met dezelfde eigenschappen als een gewoon attribuut, op een na: de naam van het attribuut komt niet voor in de Attribuut Catalogus. Het gevolg is dat er geen centrale toetsing kan zijn op de partijen die deze attributen willen uitwisselen. Met deze uitbreiding wordt het stelsel voor uitwisseling van attributen flexibel.	
(Standaard)Attribuut	Kenmerk van een Natuurlijk Persoon[6]. Een attribuut bestaat uit een *naam* en een *waarde*, en bij attribuutbronnen die dit ondersteunen, een *betrouwbaarheidsniveau* van de waarde. De naam is het label van het attribuut, en als het label voorkomt in de AC MOET de waarde van dit attribuut de betekenis reflecteren die het attribuut in de AC heeft. De naam komt voor in de AttribuutCatalogus. De waarde van het attribuut geeft de invulling die voor de persoon van toepassing is. Het betrouwbaarheidsniveau, indien beschikbaar, geeft de autoriteit weer waarmee de waarde is gezet.	SION IAA
Attribuutcatalogus (AC)	Een elektronisch bevraagbare catalogus die de gestructureerde verzameling van alle via het	AET

[5] Idensys: https://afsprakenstelsel.etoegang.nl/display/as/Startpagina
[6] Strikt genomen kunnen attributen ook kenmerken van bedrijven of, algemeen, objecten zijn, maar hier worden alleen de gevolgen van verwerking van persoonsgegevens besproken.

Begrip	Omschrijving	Bron
	netwerk verkrijgbare optionele attributen bevat inclusief de aanduiding waarmee zij opgevraagd kunnen worden.	
Authenticatie (authenticeren)	De controle (het staven) van de (een) geclaimde identiteit van een partij en de set van zijn geclaimde attributen op een bepaald betrouwbaarheidsniveau.	AET
Authenticatiedienst (AD)	Een vereiste Rol binnen het Netwerk (voor Elektronische Toegangsdiensten) die door een Deelnemer aan het Afsprakenstelsel (AS) wordt ingevuld en die de verantwoordelijkheid heeft voor het authenticeren van natuurlijke personen op basis van het door de natuurlijk persoon gebruikte Authenticatiemiddel	AET
Authenticatiemiddel	Een set van attributen (bijvoorbeeld een certificaat) op grond waarvan authenticatie van een partij kan plaatsvinden.	AET
Authenticatieverklaring	Een Verklaring waaruit het bestaan en de juistheid kan worden opgemaakt van een Authenticatie (authenticeren) die heeft plaatsgevonden in de context van een bepaalde handeling of dienst.	AET
Autorisatie	Het verlenen van toestemming (een bevoegdheid) aan een geauthenticeerde partij om toegang te krijgen tot een bepaalde dienst of toestemming om een bepaalde actie uit te voeren. Een autorisatie kan worden vastgelegd in toegangsrechten. Het verlenen van toegang kan (mede) gebaseerd zijn op die in toegangsrechten vastgelegde autorisatie.	AET
Beheerorganisatie (BO)	De Beheerorganisatie van het Afsprakenstelsel (AS) die verantwoordelijk is voor het faciliteren van het beheer en de doorontwikkeling van het Afsprakenstelsel, alsmede de controle op en het monitoren van de naleving van het Afsprakenstelsel door de Dienstverleners en de Deelnemers in opdracht van de Eigenaar.	AET
Betrouwbaarheidsniveau	Een relatief niveau van de sterkte van het bewijsmateriaal aangaande een authenticatie / identiteitsclaim, bevoegdheid, controle van bevoegdheid of wilsuiting dat wordt gevormd door een samenhangend geheel van factoren, waar van toepassing bestaande uit: de sterkte van de voorafgaande registratie, identificatie, authenticatie en uitgifte; de sterkte van het	AET

Begrip	Omschrijving	Bron
	middel zelf en het gebruik van het middel (het authenticatiemechanisme).	
Bevoegdheid	Het recht van een persoon om een handeling te verrichten.	AET
Betrouwbaarheidsniveau	Een relatief niveau van de sterkte van het bewijsmateriaal aangaande een authenticatie / identiteitsclaim, bevoegdheid, controle van bevoegdheid of wilsuiting dat wordt gevormd door een samenhangend geheel van factoren, waar van toepassing bestaande uit: de sterkte van de voorafgaande registratie, identificatie, authenticatie en uitgifte; de sterkte van het middel zelf en het gebruik van het middel (het authenticatiemechanisme).	AET
Controle van bevoegdheid	Controle van bevoegdheid zoals deze blijkt uit een in een machtigingenregister geregistreerde vertegenwoordigingsrelatie. Reden van het onderscheid tussen machtiging sec en controle van bevoegdheid is dat de machtiging ook kan bestaan los van het machtigingenregister.	AET
Dataminimalisatie	Het zodanig inrichten van een gegevensverwerking dat alleen die gegevens worden gebruikt die noodzakelijk zijn om het specifieke doel van het gegevensgebruik te bereiken. Daarmee zijn er niet meer identificerende gegevens bekend dan nodig en bovendien bij zo weinig mogelijk partijen.	AET
Deelnemer	Een partij die conform hetgeen daarover in het Afsprakenstelsel (AS) is vastgelegd één of meer rollen vervult binnen het Netwerk (voor Elektronische Toegangsdiensten). Deelnemers kunnen rollen voor eigen gebruik en/of voor gebruik door derden vervullen.	AET
Dienstafnemer	Een partij die Elektronische Toegangsdiensten gebruikt om een dienst af te nemen bij een dienstverlener. De dienstafnemer is een partij van de vorm • natuurlijk persoon die een onderneming drijft (een eenmanszaak), of • een niet natuurlijk persoon conform de identificatie waarmee het is ingeschreven in het Nederlandse handelsregister of in een vergelijkbaar buitenlands openbaar register conform de voorschriften van het betreffende land, of • een natuurlijk persoon die als privépersoon een dienst afneemt van een dienstverlener, of	AET

Begrip	Omschrijving	Bron
	• een natuurlijk persoon die als burger een dienst afneemt van een dienstverlener die gerechtigd is het BSN te gebruiken, of • een beroepsbeoefenaar Een dienstafnemer is de uitvoerende natuurlijk persoon of wordt vertegenwoordigd door een uitvoerend natuurlijk persoon.	
Dienstencatalogus (DC)	Een elektronisch bevraagbare catalogus die de gestructureerde verzameling van alle diensten, inclusief de onderverdeling in subdiensten en eventuele samengestelde diensten bevat, welke voor het vastleggen van bijzondere machtigingen, dat wil zeggen machtigingen die zich beperken tot bepaalde diensten, minimaal noodzakelijk is.	AET
Dienstverlener (DV)	Een Partij die elektronische diensten aanbiedt aan dienstafnemers waarvoor eHerkenningsdiensten voorwaardelijk zijn. Dit kan zowel een Overheids-dienst-verlener als een private Dienstverlener (DV) zijn.	AET
Gebruiker	Een onderwijsdeelnemer of ander persoon die gebruik maakt van een IAA-dienst om toegang te krijgen tot een dienst van een Service Provider. In communicatie over de gebruiker is het ook de persoon waarvan binnen het onderwijsveld gegevens tussen een Deelnemer en Service Provider wordt uitgewisseld. Deze definitie wijkt af van de definitie die bij Idensys wordt gebruikt.	AET
Geïnformeerde uitdrukkelijke toestemming	De geïnformeerde uitdrukkelijke toestemming die wordt gevraagd voorafgaand aan registratie en verstrekking van aanvullende attributen. Dit houdt in dat degene die verantwoordelijk is voor de verwerking van persoonsgegevens ervoor zorgt dat voorafgaande aan de uitdrukkelijke toestemming van de betrokkene informatie wordt verstrekt over het doel van de verwerking van persoonsgegevens, welke gegevens worden verwerkt, of er sprake is van derdenverstrekking en zo ja, met welk doel alsmede de rechten die betrokkenen tegen de gegevensverwerking kunnen uitoefenen.	AET
Gemachtigde	De partij die (op grond van wet of machtiging c.q volmacht) bevoegd is om in naam van de	AET

Begrip	Omschrijving	Bron
	vertegenwoordigde bepaalde handelingen te verrichten waarvan de rechtsgevolgen worden toegerekend aan de vertegenwoordigde. Voorzover gemachtigde een natuurlijk persoon is, geldt geen beperking ten aanzien van het voorkomen van niet ingezetenen als gemachtigde. Zo kan ook een buitenlandse natuurlijke persoon gemachtigde zijn.	
Herkenning	deze context wordt onder (electronische) herkenning verstaan: ieder van de functies van het Netwerk (voor Elektronische Toegangsdiensten) gericht op het handhaven en controleren van vertrouwen aangaande identiteiten, machtigingen, wilsuitingen en bevoegdheden in relaties of transacties tussen dienstverleners en bedrijven en de daarin betrokken uitvoerend natuurlijke personen.	AET
Herkenningsdiensten	Diensten voor Herkenning, te weten: Authenticatie (authenticeren), controle van Bevoegdheid, vastlegging van een wilsuiting en de daarbij benodigde identificaties en garanties voor onweerlegbaarheid evenals de daartoe benodigde registratieprocessen.	AET
Herkenningsmakelaar (HM)	Een vereiste Rol binnen het Netwerk (voor Elektronische Toegangsdiensten) die door een Deelnemer aan het Afsprakenstelsel (AS) wordt ingevuld en die het single point of contact vormt waarlangs dienstverleners Herkenningsdiensten afnemen, die de verantwoordelijkheid heeft om het berichtenverkeer van en naar de dienstverleners te ontkoppelen van de interne berichten binnen het netwerk en die optreedt als routeerder naar alle deelnemende authenticatiediensten, machtigingenregisters en (toekomstige) ondertekendiensten.	AET
IAA-diensten	Synoniem met Idensys Herkenningsdiensten.	SION IAA
IAA-stelsel	Synoniem met Idensys Netwerk (voor Elektronische Toegangsdiensten)	SION IAA
Identificatie (identificeren)	Het noemen van attributen van een entiteit om deze in een bepaalde context uniek aan te duiden. In de context van Elektronische Toegangsdiensten gaat het over identificatie van partijen.	AET
Identificerend kenmerk	Een reeks karakters waarmee iets of iemand (een partij) in een bepaalde context uniek wordt aangeduid. Indien het kenmerk enkel uit cijfers	AET

Begrip	Omschrijving	Bron
	bestaat wordt ook van Identificerend nummer gesproken.	
Identificerend nummer	Een Identificerend kenmerk dat bestaat uit cijfers	AET
Identiteit	De volledige maar dynamische set van alle attributen behorende bij een bepaalde entiteit die het mogelijk maakt betreffende entiteit van andere te onderscheiden. Elke entiteit heeft maar één identiteit. De identiteit behoort toe aan de entiteit.	AET
Identity provider (IdP)	Een vorm van een service provider die identiteitsgegevens aanmaakt, onderhoud en beheert ten behoeve van partijen en hen authenticeert ten behoeve van andere service providers in de context van een federatie.	AET
Intermediaire partij	Een partij die bevoegd is te handelen op grond van een aan hem verleende machtiging en die deze machtiging op grond van substitutie heeft doorgegeven aan een derde.	AET
Intern pseudoniem	Pseudoniem dat gedurende een langere periode toegepast wordt en enkel binnen Elektronische Toegangsdiensten gebruikt wordt zonder een specifiek werkingsdomein.	AET
Ketenpseudoniem	Een ketenpseudoniem is een identifier die uniek gekoppeld is aan een Gebruiker, dat gebruikt kan worden binnen een bepaalde reikwijdte. Deze reikwijdte kan begrensd zijn in tijd, handeling of tot bepaalde partijen en wordt bepaald door het Tactisch Beraad	SION IAA
Ketenverklaring	Een elektronisch vastgelegde verklaring waaruit het bestaan en de juistheid kan worden opgemaakt van een keten van bevoegdheden die aantoont dat een bepaalde uitvoerend natuurlijk persoon een bepaalde vertegenwoordigde dienstafnemer vertegenwoordigt ten behoeve van een bepaalde handeling of dienst op grond van controle van de gehele keten in machtigingenregisters	AET
Koppelregister (KR)	Een technische Rol binnen het Netwerk (voor Elektronische Toegangsdiensten) die door een Deelnemer aan het Afsprakenstelsel (AS) wordt ingevuld en die de verantwoordelijkheid heeft voor het koppelen van een (branche-specifiek) identificerend kenmerk aan het door de natuurlijk persoon gebruikte pseudoniem.	AET
Koppelvlak	Een koppelvlak is de verbinding tussen twee systemen. Om een koppelvlak te realiseren zijn nodig (a) specificaties en (b) implementaties in	AET

Begrip	Omschrijving	Bron
	mensen en middelen. Het Afsprakenstelsel (AS) levert de specificaties (a), het netwerk verzorgt de implementaties (b). Synoniem met Engelse term 'interface'.	
Machtiging (machtigen)	Een herroepbare bevoegdheid die een vertegenwoordigde verleent aan een andere partij (de gemachtigde) om in naam van eerstgenoemde rechtshandelingen te verrichten. Een machtiging kan algemeen of bijzonder zijn. Een bijzondere machtiging is beperkt tot bepaalde rechtshandelingen of een bepaalde relevante omvang ten aanzien van rechtshandelingen. Machtiging kan worden gezien als synoniem aan volmacht zij het dat de term machtiging voornamelijk in bestuursrechtelijke context wordt gebruikt.	AET
Machtigingenbeheerder	Een Uitvoerend natuurlijk persoon (UNP) met de bevoegdheid om namens een Dienstafnemer machtigingen te registreren, te schorsen, in te trekken en anderszins bijbehorende registratieprocessen uit te voeren.	AET
Machtigingenregister (MR)	Een vereiste Rol binnen het Netwerk (voor Elektronische Toegangsdiensten) die door een Deelnemer aan het Afsprakenstelsel (AS) wordt ingevuld en die de verantwoordelijkheid heeft voor het registreren, beheren, controleren van machtigingen en andere bevoegdheden en het afleggen van verklaringen over bevoegdheden (c.q. het op verzoek van de Uitvoerend natuurlijk persoon (UNP) verstrekken van machtigingsverklaringen).	AET
Machtiging-verklaring	Een elektronisch vastgelegde verklaring waaruit het bestaan en de juistheid kan worden opgemaakt van een in een geregistreerde machtiging zoals deze gecontroleerd is in een Machtigingen-register ten behoeve van een bepaalde handeling of dienst.	AET
Middelenuitgever (MU)	Een vereiste rol binnen het Netwerk (voor Elektronische Toegangsdiensten) die door een Deelnemer aan het Afsprakenstelsel (AS) wordt ingevuld en die de verantwoordelijkheid heeft voor het uitgeven van Authenticatiemiddelen conform de eisen van het gespecificeerde Betrouwbaarheidsniveau.	AET
Makelaar	Synoniem met Herkenningsmakelaar	AET

Begrip	Omschrijving	Bron
Natuurlijk persoon	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.	AET
Netwerk (voor Elektronische Toegangsdiensten)	De verzameling onderling verbonden componenten die gereguleerd worden door het Afsprakenstelsel (AS) en gezamenlijk Herkenningsdiensten leveren en daartoe bestaan uit tenminste één invulling door een Deelnemer van de rollen Herkenningsmakelaar (HM), Middelenuitgever (MU), Authenticatiedienst (AD), Machtigingenregister (MR) en BSN koppelregister (BSNk), mogelijk aangevuld met verdere rollen voor eHerkenningsdiensten zoals een ondertekendienst, hun onderlinge verbindingen, de verbindingen tot en met het koppelvlak met dienstverleners en de processen voor uitgifte van middelen, registratie van bevoegdheden en aanmelding voor hergebruik vanuit bedrijven, inclusief de benodigde voorzieningen voor beheer conform het Afsprakenstelsel.	AET
Niet Natuurlijk persoon	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.	AET
Nummergenerator	Voorziening die nummers genereerd die als identificerend kenmerk voor een gebruiker gebruikt wordt.	SION IAA
Nummervertaalvoorziening	Voorziening die identificerende kenmerken van een bepaalde gebruiker uit verschillende domeinen aan elkaar koppelt.	SION IAA
Ondertekendienst	Een (voorziene) rol binnen het Netwerk (voor Elektronische Toegangsdiensten) die door een Deelnemer aan het Afsprakenstelsel (AS) wordt ingevuld en die de verantwoordelijkheid heeft voor het doen van de wilsuiting, het valideren ervan en het verstrekken van het bijbehorende associatiebewijs.	AET
Onderwijsidentiteit	Een onderwijs identiteit (OID) is een unieke en persistente identiteit voor een deelnemer in het onderwijssector.	SION IAA

Begrip	Omschrijving	Bron
Onderwijsdeelnemer	Een Natuurlijk Persoon die gebruikt maakt van een herkenningsdienst om een dienst van een Dienstafnemer. Dit zijn bijvoorbeeld een onderwijsvolger, een vertegenwoordiger van een onderwijsvolger, of een medewerker van een onderwijsinstelling.	
Overeenkomst	De overeenkomst tussen de Dienstafnemer en de Deelnemer, of de overeenkomst tussen de Dienstverlener (DV) en de Deelnemer, op grond waarvan de Deelnemer Herkenningsdiensten verleent en waarop de Gebruiksvoorwaarden van toepassing zijn.	AET
Partij	Een persoon of samenwerkingsverband die in de context van Herkenning voorkomt of zou kunnen voorkomen en die zonodig uniek geïdentificeerd en geauthenticeerd kan worden. Voorbeelden van partijen zijn: Deelnemers, dienstverleners, bedrijven, vertegenwoordigden, gemachtigden, … De term wordt gehanteerd als generalisatie.	AET
Policy	Een lijst met regels. Voor de verstekking van attributen wordt hierin opgenomen welke Partij mag beschikken over welke gegevens en welk voorwaarden hierbij gelden.	SION IAA
Persoonsgegeven	Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.	
Privépersoon	Een Natuurlijk persoon, echter uitsluitend voor situaties en dienstafnames bij niet-overheidsdienstverleners c.q. in B2C diensten.	AET
Pseudoniem	Een arbitrair Identificerend kenmerk dat op basis van een bewerking van een ander identificerend kenmerk wordt geproduceerd op een wijze die steeds hetzelfde pseudoniem oplevert bij hetzelfde kenmerk zonder dat deze laatste herleid kan worden uit het pseudoniem. Er kunnen meerdere pseudoniemen bestaan bij één Identificerend kenmerk, ieder met een eigen werkingsdomein. In dat geval zijn twee pseudoniemen van hetzelfde kenmerk in verschillende domeinen niet aan elkaar te relateren.	AET
Sectoridentiteit	Een (branche-specifiek) identificerend kenmerk dat aan het pseudoniem van een natuurlijk persoon gekoppeld is via het Koppelregister.	
Service provider (SP)	Een rol die vervuld wordt door een afgebakend en actief onderdeel van een systeem dat diensten aanbiedt aan partijen of aan andere onderdelen	SION IAA

Begrip	Omschrijving	Bron
	van dat systeem. In dit document wordt dit beperkt tot een Dienstafnemer (Partij die een IAA-dienst afneemt om een Onderwijsdeelnemer toegang te kunnen verschaffen tot een elektronische dienst.	
Single Sign On (SSO)	Een functie die wordt gefaciliteerd zoals omschreven in het Afsprakenstelsel (AS), waardoor een authenticatie van een uitvoerend natuurlijk persoon wordt hergebruikt, waardoor deze uitvoerend natuurlijk persoon niet opnieuw hoeft in te loggen.	AET
Specifiek pseudoniem	Pseudoniem dat gedurende een langere periode toegepast wordt in een specifiek werkingsdomein. Een dienstverlenerspecifiek pseudoniem is steeds hetzelfde voor dezelfde Dienstverlener (DV) in wiens context het gebruikt wordt, een dienstafnemerspecifiek pseudoniem is steeds hetzelfde voor de context van één dienstafnemer etc.	AET
STORK (2)	Secure idenTity acrOss boRders linKed. *www.**eid-stork2**.eu*	SION IAA
Tactisch Beraad (gremium)	Het tactische overleg aangaande beheer van het Afsprakenstelsel, dat wordt georganiseerd door de beheerorganisatie.	SION IAA
Toegang verlenen	Een proces onder verantwoordelijkheid van de dienstverlener waarin op grond van door Elektronische Toegangsdiensten verstrekte verklaringen en mogelijke controles van andere relevante toegangsrechten die door de dienstverlener zelf zijn vastgelegd bepaald wordt of een uitvoerend natuurlijk persoon toegang krijgt tot een bepaalde dienst of gerechtigd is een bepaalde actie uit te voeren.	AET
Toezichthouder	De toezichthouder ziet toe op de veilige en betrouwbare werking van het Afsprakenstelsel (AS).	AET
Uitvoerend natuurlijk persoon (UNP)	Een Natuurlijk persoon die namens een Dienstafnemer handelt (die dienstafnemer heet dan: vertegenwoordigde dienstafnemer) op basis van een bevoegdheid tot vertegenwoordiging van die dienstafnemer. In het kader van eHerkenning betreft dit handelen het afnemen van een dienst bij een dienstverlener.	AET
User consent	De geïnformeerde uitdrukkelijke toestemming die wordt gevraagd voorafgaand aan registratie en verstrekking van aanvullende attributen. Dit houdt in dat degene die verantwoordelijk is voor	AET

Begrip	Omschrijving	Bron
	de verwerking van persoonsgegevens ervoor zorgt dat voorafgaande aan de uitdrukkelijke toestemming van de betrokkene informatie wordt verstrekt over het doel van de verwerking van persoonsgegevens, welke gegevens worden verwerkt, of er sprake is van derdenverstrekking en zo ja, met welk doel alsmede de rechten die betrokkenen tegen de gegevensverwerking kunnen uitoefenen.	
Verklaring	Een elektronisch vastgelegd bericht dat gevraagde identiteitsinformatie en attributen bevat conform de koppelvlakspecificaties en waarvoor een bepaalde Deelnemer aantoonbaar instaat. Afhankelijk van de betreffende identiteitsinformatie wordt gesproken van een authenticatieverklaring, een machtigingsverklaring of een Ketenverklaring. Een verklaring kan andere verklaringen omvatten en voor de aantoonbaarheid vereisen, dan wordt gesproken over een verklaring over x en y waarbij de wijze waarop de verklaringen in elkaar grijpen in detail in de Interface specifications is beschreven.	AET
Vertegenwoordigde	De partij die de vertegenwoordiger de bevoegdheid heeft verleend om in naam van eerstgenoemde te handelen.	AET
Vertegenwoordigde dienstafnemer	Dienstafnemer die niet zelf handelt maar zich laat vertegenwoordigen. De vertegenwoordigde dienstafnemer is de eerste partij in een keten van machtigingen.	AET
Vertegenwoordiger	De Partij die bevoegd is om een andere partij (de vertegenwoordigde) te vertegenwoordigen in het verrichten van handelingen met derden.	AET
Vertegenwoordiging (vertegenwoordigen)	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	AET

Begrip	Omschrijving	Bron
	een bepaalde relevante omvang ten aanzien van rechtshandelingen. In privaatrechtelijke context wordt naast het begrip vertegenwoordiger, agent of gevolmachtigde gehanteerd in plaats van gemachtigde.	
Wettelijke vertegenwoordiging	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.	AET
Wilsuiting	Een wilsuiting is een elektronische handtekening die de elektronisch vastgelegde gegevens waarop de wilsuiting betrekking heeft, verbindt met de elektronische gegevens op basis waarvan de Uitvoerend natuurlijk persoon (UNP) die de wilsuiting afgeeft op ieder moment nadien geauthenticeerd kan worden.	AET

5 Referenties

[1] Idensys Afsprakenstelsel ETD 1.9b

[2] SION IAA Architectuurdocument versie 0.7

[3] Privacyconvenant ####

[3] Dataverzameling boek ####