edustandaard

Memo

Voor:	Standaardisatieraad, Edustandaard
Van:	Bram Gaakeer (namens de Architectuurraad Edustandaard)
Datum	03-05-2017
Betreft	Voorstel voor inventarisatie en opstellen overzicht IAA

1. Inleiding

In de huidige situatie is binnen het onderwijsdomein de wijze van identificeren en authentiseren van natuurlijke en niet-natuurlijke personen, bijvoorbeeld ten behoeve van toegang, afhankelijk van doelgroep, proces en sector. Dit is inefficiënt en maakt het ook lastig om flexibel om te kunnen gaan met de steeds sneller veranderende wereld. Er worden steeds hogere eisen aan identificatie en authenticatie gesteld. Zo wordt er ook vanuit de centrale overheid in het kader van de wet GDI steeds meer gestuurd op het hergebruik van centrale voorzieningen en (technische) interoperabiliteit. Op dit moment is voor het onderwijsdomein, hoewel er binnen o.a. het SION-programma wel aan gewerkt is, nog geen gemeenschappelijk, door iedereen onderschreven toekomstbeeld voor identificatie en authenticatie. Wel zijn er in de sectoren en in processen veel initiatieven die gericht zijn op vernieuwing van identificatie, authenticatie en autorisatie (IAA) waarbij standaardisatie een belangrijke rol kan spelen. Het is wenselijk om deze initiatieven met elkaar te vergelijken en de gemeenschappelijke aspecten inzichtelijk te maken als eerste stap richting een mogelijk gemeenschappelijk afsprakenstelsel.

In de Architectuurraad van 13 april 2017 is in dit kader aandacht besteed aan de invoering van de wet GDI. De eerste tranche van die wet beschrijft onder andere welke eisen worden gesteld aan de digitale diensten van organisaties met een publieke taak ten aanzien van identificatie en authenticatie van burgers en bedrijven.
Ook is de notitie besproken die Jan Bartling op 13 januari 2017 heeft gestuurd aan de Standaardisatieraad waarin hij een voorstel doet om met een aanpak te komen die er op is gericht de eerste stap te zetten op weg naar een gemeenschappelijk toekomstbeeld ten aanzien van identificatie en authenticatie in het onderwijs. Hij pleit daarin voor:

1. Inventarisatie & overzicht (uiteindelijk in heldere taal).
2. Kennissessies organiseren voor bestuurders – doelgroep: instellingen PO t/m WO, en ook OCW.
3. Dilemma's & knelpunten-op-bestuurlijk-niveau vaststellen en hierover de discussie en visievorming faciliteren. Ook de principes vaststellen ter ondersteuning van de visie.
4. Met de opbrengsten sturing geven richting Informatiekamer en andere bepalende organen. Ook richting het architectuur denken.

Hiervoor is voorwerk nodig, er moet een beeld zijn van de huidige situatie en de daarbij horende (bestuurlijke) dilemma's. Stap 1 past zijns inziens binnen Edustandaard; voor de vervolgstappen moet worden bekeken welke rol Edustandaard kan hebben.

De Architectuurraad heeft op basis van beide behandelde onderwerpen geconcludeerd dat de tijd rijp is om een overkoepelende baseline voor IAA te ontwikkelen vanuit Edustandaard en die te koppelen aan de ROSA. De behoefte van Jan Bartling aan een inventarisatie wordt breed gedeeld. De wereld om ons heen verandert en er zijn veel initiatieven om de toegang te verbeteren. Het is cruciaal om vast te stellen of deze initiatieven op elkaar aansluiten en voldoende zijn om te voldoen aan de veranderende eisen.Die baseline kan dienen voor verdere visievorming die in andere contexten zal moeten plaatsvinden, Edustandaard zou hiervoor de ingrediënten moeten aandragen. Het is ook écht de rol van de Architectuurraad om zich voor het scheppen van inzicht en overzicht hard te maken. Er is derhalve besloten om een opdrachtomschrijving op te stellen en de opdrachtgevers / belanghebbenden te mobiliseren – te starten bij de Standaardisatieraad. Sir Bakx (Surf) geeft nog mee dat voor goede acceptatie de baseline dekkend moet zijn voor alle doelgroepen – anders blijven partijen huiverig om in te stappen. Verder is benadrukt dat het noodzakelijk is om qua timing goed rekening te houden met alle lopende en opstartende ontwikkelingen in dit domein.

De Architectuurraad doet middels deze notitie een voorstel voor de uitvoering van de inventarisatie.
Ingegaan wordt op:

- Doelgroep
- Aandachtsgebieden inventarisatie;
- Scope;
- Aanpak en planning.

2. Aandachtsgebieden inventarisatie

Doelgroep

De inventarisatie kent qua doelgroep een tweetrapsraket. Eerst moet op architecturaal niveau de uitwerking plaatsvinden, met dit onderwerp ontkomen we er niet aan dat de eerste uitwerking nog redelijk inhoudelijk/technisch zal zijn. Echter, gegeven ook de wens die Jan Bartling heeft geuit, moet die uitwerking uiteindelijk op het niveau van bestuurders worden gepresenteerd. Zij moeten inzicht krijgen wat de problemen en overwegingen zijn. Een dergelijke vertaalslag vraagt aandacht voor de inrichting van het werk en de partijen/mensen die daaraan bij moeten dragen.

Identiteiten

Identiteiten spelen een belangrijke rol bij toegang. Op basis van onder meer de identiteit kan worden bepaald welke rechten een persoon heeft bij de toegang. Dezelfde persoon kan verschillende identiteiten hebben. Onder andere door ketensamenwerking ontstaat steeds meer behoefte aan federatieve oplossingen voor uitwisselen van identiteiten. Privacybeschermende maatregelen zijn hier onderdeel van, zoals pseudonimisering. Dit vereist een infrastructuur en afspraken die dit ondersteunen en deze zijn hiermee randvoorwaardelijk.

Bij de inventarisatie moet in ieder geval rekening worden gehouden met de identiteiten van:

- Bevoegd gezag,
- Onderwijsaanbieder;
- Nederlandse burger (BSN);
- Europese student (Uniqueness ID);
- Internationale student;
- Onderwijsdeelnemer < 16 jaar)
- Onderwijsdeelnemer > 16 jaar;
- Leraar (BSN);
- Onderwijspersoneel;
- Onderzoeker;
- Europese onderzoeker (Uniqueness ID);

- Internationale onderzoeker;
- Ouder.

Tevens moet gekeken worden naar het gebruik van pseudonimisering. Hierbij wordt gekeken naar zowel de vormen zoals polymorfe pseudoniemen (eID) en het ketenpseudoniem (voor bestellen en gebruik digitale leermiddelen) als hun bereik.

Authenticatiemiddel

Bij authenticatie wordt de identiteit van een gebruiker vastgesteld met een authenticatiemiddel.
Hierbij wordt onderscheid gemaakt in beveiligingsniveaus (laag, substantieel en hoog). Uitgangspunt is dat de gebruiker zelf een erkend middel kan kiezen waarbij dit middel voldoet aan het beveiligingsniveau dat de dienstaanbieder vereist. De gebruiker kan het middel kiezen omdat er in de infrastructuur meerdere middelen beschikbaar zijn (multi-middelen strategie). Het beveiligingsniveau dat diensten vereisen zal de komende tijd in beweging komen door nationale en Europese ontwikkelingen (eIDAS[1]). Daarom moet het toekomstbeeld toegang er rekening mee houden middelen die geboden worden vanuit DigiD (substantieel), iDIN en Idensys. Hierbij wordt vooral gekeken bij welke processen behoefte is aan deze middelen.

Attribuutproviders

Naast identiteiten zijn vaak attributen nodig bijvoorbeeld ten behoeve van gebruiksgemak/ervaring of de autorisatie. Attributen worden verstrekt door een attribuutprovider. Daarbij kan aan allerlei vormen van informatie worden gedacht. Belangrijk aandachtspunt hierbij is hoe de user consent hierbij geregeld wordt.

Autoriseren

Bij toegang moet het mogelijk zijn om op basis van de rol van een persoon te bepalen welke toegang deze persoon mag hebben tot gegevens en diensten. Dit is vaak nauw verweven met een attribuutprovider. Dit hoeft echter niet. Bijvoorbeeld bij Idensys is er sprake van machtigingenregister waarbij een bevoegd bezag middels natuurlijke personen toegang kan geven tot specifieke diensten.

3. Scope

Op dit moment lopen 3 belangrijke initiatieven in het onderwijs. Ons voorstel is om de inventarisatie hier op verder laten gaan door deze initiatieven met elkaar in verband te brengen om de gemeenschappelijke aspecten (principes, ontwerpkaders, IAA-patronen voor processen etc, oplossingsrichtingen, best-practices) inzichtelijk te maken, maar ook de “gaps’ en de mogelijke tegenstrijdigheden. Deze 3 initiatieven geven inzicht op een deel van het gewenste toekomstbeeld:

1. **Inventarisatie eID**
   Een reeds uitgevoerde inventarisatie wordt verder voortgezet. Hierbij zijn er 2 aandachtsgebieden:
   - Hoe wordt omgegaan met onderwijsnummer;
   - Mogelijkheid om Idensys/eHerkenning te gebruiken voor authenticatie onderwijspersoneel;
2. **Inventarisatie contentketen PO, VO en MBO**
   Op basis van een in Edu-k opgesteld functioneel toekomstperspectief op toegang en IAA wordt door Innovalor een nadere uitwerking van dit toekomstperspectief uitgevoerd alsmede een toetsing op de technische, organisatorische en juridische haalbaarheid ervan;;
3. **Inventarisatie SURF**
   Voor het primaire proces van HO vervult de SURF federatie de rol van identy en attribuut provider. Voor HO is het van belang om vast te stellen of de toegang voor het primaire proces en voor de

[1] http://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32015R1502&from=EN

administratieve processen op elkaar gaan aansluiten of dat dit gescheiden werelden blijven. De Wiki met identiteiten zal worden gebruikt om vast te stellen welke identiteiten er zijn en op welke wijze ze gedeeld worden.

Als duidelijk is of deze toekomstbeelden op elkaar aansluiten levert dit al een belangrijke indicatie of het mogelijk is om een gezamenlijk toekomstbeeld voor IAA voor het volledige Onderwijsdomein te schetsen.

3.1. eID

Rijksbreed loopt het eID programma. De eerste tranche richt zich vooral op identificatie en authenticatie van natuurlijke personen, in combinatie met pseudonimisering. Aangekondigd is dat hierna authenticatie van niet-natuurlijke personen en machtigen worden opgepakt. Binnen het eID stelsel is ook uitgewerkt hoe omgegaan wordt met authenticatie van burgers uit andere EU-landen (eIDAS).
In het kader van de wet GDI heeft voor eID een procesinventarisatie plaatsgevonden bij alle onderwijssectoren. Voor verschillende ketens (aanmelden/inschrijven, examineren, secundaire processen, primair proces) is in kaart gebracht wat de consequenties van eID zijn. De eerste processen waarbij aangesloten moet worden op eID zijn studiefinanciering en inschrijven van studenten in het HO. Een aandachtspunt is hoe omgegaan wordt met onderwijsdeelnemers zonder BSN.
Voor fase 2 wordt gekeken of onderwijspersoneel gebruik kan maken van eID/Idensys. Aandachtspunt is de wijze van autorisatie icm met machtigen of mandateren. Idensys autoriseert per Bevoegd Gezag op het niveau van diensten. Een belangrijk raakvlak heeft dit onderwerp met het streefbeeld H2M2M, dat in 2016 is opgesteld door OCW, DUO, de onderwijsraden PO en VO, VDOD en Kennisnet. Daarin is onderkend dat autorisatie bij toegang rechtstreeks tot een dienst (bijv. Zakelijk portaal van DUO) vanuit een onderwijsinstellingen door een daartoe gerechtigde medewerker maar 1 kant is die speelt bij de toegang van niet-natuurlijke personen, maar dat dit ook geldt voor gegevensuitwisseling die deze medewerker via een machine-to-machine koppeling laat uitvoeren (al of niet via een SaaS-leverancier). Het moet ook mogelijk zijn om te regelen dat toegang wordt verstrekt tot gegevens van een specifieke school.

3.2. Toegang in de contentketen (PO, VO, MBO)

Edu-K heeft een werkgroep ingericht, die een functioneel toekomstperspectief toegang heeft opgeleverd. Dit toekomstperspectief wordt door Innovalor nader uitgewerkt en getoetst op technische, organisatorische en juridische haalbaarheid. Dit omvat een (functioneel) ontwerp van het toekomstig toegangs- en attributenstelsel. Dit stelsel moet scholen docenten, leerlingen en studenten in staat stellen veilig, betrouwbaar en efficiënt via Single Sign-On toegang te bieden tot (alle) educatieve diensten. In dit toekomstbeeld moet het mogelijk zijn om externe identiteiten van gebruikers te kunnen koppelen aan de identifiers die binnen de eigen federatie worden gebruikt. Dit betekent dat aansluiting mogelijk is met de identiteiten die binnen het eID-stelsel worden gebruikt. Innovalor rapporteert haar bevindingen in juni 2017.

3.3. Inventarisatie HO

SURF heeft een wiki met een overzicht van ca. 50 identiteiten of projecten/activiteiten. Dit zal gebruikt worden om vast te stellen welke identiteiten er zijn. Vervolgens wordt gekeken welke beelden er binnen het HO bestaan voor de uitwisseling van deze identiteiten, zowel voor het administratieve domein als voor het primair proces.

4. Voorgestelde aanpak

Stap 1: Samenstellen van een werkgroep IAA
Onder Edustandaard wordt een werkgroep geformeerd met daarin afgevaardigden van zowel publieke als private organisaties. De precieze afvaardiging is aan de Standaardisatieraad, maar het ligt in de lijn der verwachtingen dat minimaal OCW, DUO, Surf, saMBO-ICT en Kennisnet namens de publieke sector actief zullen deelnemen en dat vanuit de private sector vertegenwoordigers namens de uitgevers (GEU), LAS/SIS-leveranciers (VDOD) en de distributeurs deelnemen. Te denken valt aan leden van de Architectuurraad Edustandaard, maar omdat het resultaat niet alleen gericht moet zijn op architectuur en techniek maar (juist) ook geschikt moet zijn voor een bestuurlijke insteek, is inbreng van een meer beleidsmatig perspectief wenselijk om die vertaalslag te kunnen maken.
Praktisch gezien is het aannemelijk om vanuit de werkgroep een subgroep te formeren met daarbij in ieder geval een architect/standaardisatie-expert van Bureau Edustandaard om veel inhoudelijk (voor)werk verrichten, de andere leden van de werkgroep kunnen dan input leveren en reviewen. Uiteindelijk is de gehele werkgroep eindverantwoordelijk voor de oplevering van de afgesproken resultaten.

Stap 2: Overzicht en analyse inventarisatie van de resultaten van de drie genoemde initiatieven
Deze werkgroep gaat de resultaten die uit de hierboven genoemde initiatieven zijn voortgekomen inventariseren en daarvan een overzicht opstellen. Op basis van het overzicht worden de overeenkomsten en verschillen geduid, gemeenschappelijke principes opgesteld en worden de blinde vlekken en tegenstrijdigheden benoemd. Het overzicht wordt vertaald naar een voor bestuurders hanteerbare vorm en inhoud.

Te overwegen valt om op basis van stap 2 een voorstel op te stellen voor vervolgstappen, bijvoorbeeld het opstellen van een afsprakenstelsel IAA, bestaande uit een bestuurlijk deel en een architectuurdeel.
Indachtig de notitie van Jan Bartling, is het de vraag of de uitvoering hiervan dan bij Edustandaard moet liggen. Voor het uitwerken van de architectuur en dit verwerken in de ROSA ligt dit in de lijn der verwachtingen, voor de andere genoemde stappen in Jan Bartlings notitie zijn er eerder andere invullingen denkbaar.

5. Globale planning

Het volgende lijkt voorlopig haalbaar:

1. Opdracht geven aan de Architectuurraad door de Standaardisatieraad tot het formeren van een werkgroep met hierboven beschreven taak (13 juli 2017).
2. Samenstelling werkgroep (met behulp van directe inbreng en commitment vanuit de leden van de Standaardisatieraad). Gegeven de zomervakantie: eind augustus.
3. Inventarisatie uitvoeren bij de genoemde initiatieven en die bespreken in werkgroep en uiteindelijk opleveren van het overzicht en de analyse. Doorlooptijd: september t/m november afhankelijk of het mogelijk is om de werkgroep minimaal 2 tot 3 keer in die periode bij elkaar te brengen om de tussen- en eindresultaten te bespreken. Het is uiteraard mogelijk om tussentijds wel over de voortgang te rapporteren als daar vraag naar is en ook ruimte voor is.

hankelijk of de opdracht ook wordt gegeven voor het opstellen van een voorstel voor vervolgstappen bijvoorbeeld de uitwerking afsprakenstelsel IAA., zou deze stap wel in de genoemde periode parallel opgestart kunnen worden in november en de oplevering van het voorstel eind december/begin januari.

Aandachtspunten:

- De leden van de Standaardisatieraad wordt gevraagd om te zorgen dat een vertegenwoordiger van de eigen organisatie deel neemt aan de werkgroep. Het gaat om een technisch onderwerp het is belangrijk dat de vertegenwoordiger kennis heeft van identificatie en authenticatie en de wijze waarop deze in hun eigen domein wordt toegepast. De doorlooptijd van de inventarisatie wordt mede bepaald door de geleverde inzet. Wanneer extra middelen beschikbaar worden gesteld voor externe ondersteuning kan het project versneld worden;
- De organisatie Innovalor heeft een concept eindrapport uitgebracht. Voor de planning wordt er van uitgegaan dat Edu-K voor augustus een definitief rapport goedkeurt.