Verslag werkgroep Toegang

Aanwezig: Peter Clijsters (SURF), Tom van Veen (SURF), Dirk Linden (Kennisnet), Paul de Wit (saMBO-ICT/MBO Raad), Freek Nabuurs (Cito), Bram Gaakeer (OCW, voorzitter), Erwin Reinhoud (Kennisnet, Bureau Edustandaard)

Afwezig: Edwin Verwoerd (KBb-E), Brian Dommisse (Kennisnet, PO/VO-raad), Frits Bouma (DUO), Jan Over (SURF/HOSA),

Datum
23 september 2021

Agenda

1. Opening en mededelingen
2. Vaststellen verslag vorig overleg en actiepunten
3. Verslag 26 augustus 2021 & acties
4. Vervolg ROSA scan kaders (principes)
5. Terugkoppeling OCW themabijeenkomst Digitale Identiteiten

1. Opening en mededelingen

Agenda wordt zonder wijzigingen vastgesteld.

2. Vaststellen verslag en actiepunten

2.1. Verslag

Het verslag van 26 augustus wordt zonder wijzigingen vastgesteld

2.2. Actiepunten

Actiepunt #5 Voorstel om aanpak uit te breiden met autorisatie rollen en het proxy model (Erwin)

- Geen voorderingen

Actiepunt #6 (verslag 18 maart) Uitwerken use case / probleemstelling toegang bij meerdere onderwijsinstellingen (Paul)

- Agendapunt, presentatie door Paul

Actiepunt #8: Kaders voor thema toegang ontwikkelen tbv ROSA scan. (Bram/Erwin)

- Agendapunt (combi met #15)

Actiepunt #11:Nieuwe versie GO I&A-Machtigen op Drive plaatsen (Frits)

- Zodra er een nieuwe versie beschikbaar is wordt deze op drive geplaatst

Actiepunt #13: Nagaan welke doelen er nu in een ARP opgenomen zijn (Erwin)

- Uitgevoerd

Actiepunt #14: voorbeeld verwerkersovereenkomst opleveren (Freek)

- Uitgevoerd, is in map geplaatst, maar moeten we nog uitwerken in tabel
- Volgende keer overzicht bespreken

Actiepunt #16: GEU vragen om vervanger Rimmer (Bram)
- Uitgevoerd, navraag gedaan, nog geen antwoord

Actiepunt #17: Edu-K casus achternaam delen met leden (Edwin)
- Geen vorderingen

3. Attributen en doelbinding (actiepunten #12/13)

Aan het attributenoverzicht van de federaties is nu een voorbeeld opgenomen op basis van een ARP. Dit laat zien dat onze huidige indeling van attributen ook redelijk overeenkomt met wat nu in een ARP als doel is opgegeven. Het is echter een voorbeeld en er is nog geen duidelijkheid in hoeverre alle ARP's een vergelijkbare vulling hebben. We hebben nu in ieder geval meer inzicht welk doel bij een bepaald attribuut hoort. We stellen dat het bij de federaties (toegang/authenticatie) met name moet gaan om identificerende attributen en attributen die voor de autorisatie worden gebruikt. De attributen rond display, business data en communicatie zouden in principe alleen ad hoc in een bepaalde context geleverd (of opgehaald) moeten worden (zoals Edu-K casus achternaam). Bij attributen van het type 'display' kan men stellen dat deze valide zijn omdat het gebruikelijk is om de dienstafnemer na het inloggen een herkenbare omgeving te bieden. Maar attributen die onder dit doel vallen zouden zeer beperkt moeten zijn (bijvoorbeeld een roepnaam/voornaam). Dienstaanbieders die over gegevens van het type 'business data' willen beschikken zullen (per geval) mogelijk verschillende doelen hanteren en maakt het verder generaliseren lastig (business data kan bijvoorbeeld ook reclame als doel hebben).

De volgende stap is om ook de attributen en doelen uit een verwerkingsovereenkomst op te nemen. Dit bespreken we een volgende keer. We hopen hierna dan een duidelijker beeld te hebben welke attributen bij toegang verwacht mogen worden en welke specifiek zijn in bepaalde context. Voor deze laatste moet het doel door de dienstaanbieder geformuleerd worden en moet door de leverende partij kritisch geëvalueerd worden. Hiervoor biedt SURF nu ook al een stappenplan[1].

Actiepunt #13 is afgehandeld.

4. Use case / probleemstelling toegang onderwijsinstellingen (actiepunt #6)

Aan de hand van een presentatie[2] wordt de probleemstelling toegelicht. De probleemstelling heeft ook een relatie met use cases 1b en 1c.

Er zijn verschillende ontwikkelingen binnen het mbo. Er zijn o.a. meer en meer samenwerkende ROC onderwijsinstellingen die gezamenlijk een opleiding aanbieden, er vindt vaker onderwijs op afstand plaats en een leven lang ontwikkelen wordt een steeds belangrijker thema.

Toegang is momenteel vaak ingericht vanuit het perspectief van de onderwijsinstelling. Deze voert het Identiteitenbeheer en authenticatiemiddelenbeheer uit. Vanuit het perspectief van de student resulteert dit in het gebruik van meerdere authenticatiemiddelen (accounts) die alleen toeging bieden aan diensten/systemen van de betreffende onderwijsinstelling. Bij een samenwerkingsverband staat de student slechts bij één van de onderwijsinstellingen

[1] Identity provider aansluiten op SURFconext - SURFconext - Get Conexted - SURF Wiki (surfnet.nl)
[2] Zie use case op drive: https://drive.google.com/drive/folders/1vyiNluPB725hzB5C1vLMfhLdRPhRyDYK?usp=sharing

ingeschreven. Bij de andere wordt de student dan vaak gezien als gast waar extra voorzieningen voor moeten getroffen. Afhankelijk van de situatie worden er door beide onderwijsinstellingen ook onnodig dezelfde licenties voor de student beschikbaar gesteld.

Vanuit de student gezien (die mogelijk thuis werkt met eigen device) is het ook lastig te bepalen op basis van welke criteria welke account moet worden gebruikt om in te loggen. Als de WYF in cookies is opgeslagen wordt hier mogelijk al automatisch een keuze in gemaakt (maar is dat de juiste?).

Wat is een mogelijke oplossing voor dit probleem? Er is een verschuiving van perspectief wenselijk, toegang moet niet vanuit het perspectief van de onderwijsinstelling georganiseerd worden, maar vanuit de student. De student moet met zijn eigen device en authenticatiemiddel kunnen inloggen op diensten/systemen van beide onderwijsinstellingen, waarbij, indien van toepassing, er slechts 1 licentie voor een bepaalde dienst beschikbaar is gesteld.

De oplossing voor het probleem heeft vanwege andere zaken wel een lagere prioriteit gekregen. Wat concreet gedaan moet worden om het probleem op te lossen is nu nog niet bekend. De probleemstelling wordt toegevoegd aan de use case 1c (actiepunt #18).

5. Inventarisatie principes

De bestaande SURF principes[3] worden gepresenteerd als vertrekpunt. Er wordt geconcludeerd dat de principes voor een groot deel passen, maar vanuit de context van SURF zijn opgesteld. Voor de volgende keer worden er principes opgeteld door Bram en Erwin (actiepunt #8).

6. Rondvraag & afsluiting

We hebben het laatste agendapunt (terugkoppeling OCW themabijeenkomst Digitale Identiteiten) niet kunnen bespreken. Het verslag van deze bijeenkomst is op de drive geplaatst zodat leden dit eventueel zelf kunnen nalezen.

Het volgende overleg is op 21 oktober 2021 van 15:00 tot 17:00 uur. Op de agenda staan dan de volgende onderwerpen:

- Mededelingen en opening
- ROSA scan principes
- ..

7. Actielijst

#	Omschrijving	Status	Einddatum	Actie-houder
5	Voorstel om aanpak uit te breiden met autorisatie rollen en het proxy model	Open		Erwin
6	Uitwerken use case / probleemstelling toegang bij meerdere onderwijsinstellingen	Uitgevoerd		Paul (en Peter)
8	Kaders voor thema toegang ontwikkelen tbv ROSA scan. We beginnen met principes en we gaan bij voorkeur gebruik maken van bestaande principes voor toegang	Loopt		Bram en Erwin

[3] https://www.surf.nl/visie-iaa-belangrijkste-trends-identiteitsstelsels

11	Nieuwe versie GO I&A-Machtigen op Drive plaatsen	Open		Frits
13	Nagaan welke doelen er nu in een ARP opgenomen zijn. Analyse of deze doelen overeenkomen met doelen van actiepunt #12	Uitgevoerd		Dirk
14	Voorbeeld verwerkersovereenkomst opleveren	Open		Freek
16	GEU vragen om vervanger Rimmer	Open		Bram
17	Edu-K casus achternaam delen met leden	Open		Edwin
18	Probleemstelling toegang onderwijsinstellingen opnemen bij use case 1c	Open		Erwin

BES = Bureau Edustandaard
Grijs = afgehandeld of vervallen