Verslag werkgroep Toegang

Aanwezig: Brian Dommisse (Kennisnet, PO/VO-raad), Peter Clijsters (Surfmarket), Frits Bouma (DUO), Tom van Veen (Surfmarket), Dirk Linden (Kennisnet), Freek Nabuurs (Cito), Rimmer Hylkema (Thiememeulenhoff, GEU), Jan Over (SURF/HOSA), Bram Gaakeer (OCW, voorzitter), Erwin Reinhoud (Kennisnet, Bureau Edustandaard)

Afwezig: Edwin Verwoerd (KBb-E), Paul de Wit (saMBO-ICT/MBO Raad)

Datum
20 mei 2021

Agenda

1. Opening en mededelingen
2. Vaststellen verslag vorig overleg en actiepunten
3. Probleemstelling toegang bij meerdere onderwijsinstellingen(actiepunt #6)
4. Use cases rond onderwijs federaties (actiepunt #7)
5. Gemeenschappelijke Overheidsarchitectuur (Machtigen, I&A, Gegevensuitwisseling)
6. Visie op digitale identiteit (actiepunt #9)
7. Notitie ROSA scan architectuurkaders (actiepunt #8)

1. Opening en mededelingen

Agendapunt 3 Probleemstelling toegang bij meerdere onderwijsinstellingen (actiepunt #6) wordt een andere keer behandeld als Paul aanwezig is.

Agendapunt 5 (Gemeenschappelijke Overheidsarchitectuur) komt een volgende keer. Er is nog geen nieuwe versie beschikbaar (zie actiepunt #11)

Agendapunt 6 wordt samen met agendapunt 7 besproken. Een aantal belangrijke elementen uit de Visie op digitale identiteit zijn opgenomen in de ROSA scan architectuurkaders.

2. Vaststellen verslag en actiepunten

2.1. Verslag

Het verslag van 20 april wordt zonder wijzigingen vastgesteld

2.2. Actiepunten

Actiepunt #5 (verslag 18 februari) Voorstel om aanpak uit te breiden met autorisatie rollen en het proxy model

- Loopt, geen vorderingen

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

- Loopt, geen vorderingen

Actiepunt #7 (verslag 18 maart) Use cases rond onderwijs federaties

- Agendapunt, actiepunt afgehandeld

Actiepunt 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

- Agendapunt.

Actiepunt 9: Wat willen we de informatiekamer meegeven mbt de Visie op digitale identiteit van BZK

- Agendapunt, enkele onderdelen van visie zijn al opgenomen in notitie (zie actiepunt 8), actiepunt afgehandeld

Actiepunt 10: Wat kunnen wij eventueel van de BZK visie overnemen (in verschillende referentie architecturen waarin het thema toegang is opgenomen)

- In ROSA scan notitie is e.e.a. overgenomen (zie actiepunt 8), actiepunt afgehandeld

Actiepunt 11:Nieuwe versie GO I&A-Machtigen op Drive plaatsen

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

3. Use cases rond onderwijs federaties (actiepunt #7)

Al eerder hebben we de volgende use cases rond de federaties gedefinieerd:

1. UC1 – Federatieve toegang, wat zijn de verschillen tussen sectoren (Kennisnet Entree / SURFconext).
2. UC2 – Huidige confederatie tussen EF en SURFconext
3. UC3 - Diensten die producten voor lerarenopleiding aanbieden

Bij de derde use case is nog niet helemaal duidelijk waarom deze apart onderkent wordt. Mogelijk worden er bij toegang tot diensten voor een lerarenopleiding specifieke identifiers of attributen gebruikt. Voorlopig wordt de derde use case niet verder uitgewerkt.

Peter geeft een presentatie rond de eerste twee use cases.

UC1 – Federatieve toegang (Entree Federatie/ SURFconext)

De eerste use case betreft eigenlijk een analyse van verschillen en overeenkomsten tussen de twee federaties. Hierbij gaat het om het volgende:

1. ARP overeenkomst
2. Identifiers
3. Attributen
4. Schema's
5. Autorisaties

ARP overeenkomst

De Attribute Release Policy overeenkomst wordt met verschillende rollen afgesloten:

- Entree Federatie heeft een ARP tussen dienstaanbieder en school. Entree Federatie levert altijd een bepaalde set attributen aan aangesloten dienstaanbieders. Alleen voor de aanvullende set is een ARP[1] noodzakelijk.
- SURFconext heeft een ARP tussen SURFconext en dienstaanbieder

[1] KNF:Attributen overzicht voor Service Providers - Kennisnet Developers Documentatie

Dit verschil speelt in de huidige situatie. Op termijn lijken de federaties beide een ARP tussen Federatie en dienstaanbieder te gaan toepassen. Hiermee zitten beide in vergelijkbare rollen, de federatie levert de gegevens aan de dienstaanbieder en heeft hierover een overeenkomst. Bij SURFconext hebben de scholen (IdP/Authenticatiedienst) een afspraak met SURFconext binnen de abonnement constructie.

Identifiers
Volgens de definitie van in de aanpak is een identifier een label (meestal een string of tekst) waarmee je een entiteit (een persoon, object o.i.d.) aanduidt. Dit kan dus eigenlijk als een bepaald type attribuut gezien worden. Deze benoemen we echter wel apart omdat er enerzijds vaak in de standaarden een identifier onderkend wordt (SAML-NAMEID/OIDC claim) en anderzijds de authenticatieverklaring deze verbind aan een bepaald betrouwbaarheidsniveau.

- Entree Federatie levert een shared id in de NAMEID (hash(userId)@realm), dit is een hash van de identifier die van de IdP/Authenticatiedienst komt.
- SURFconext levert een targeted identifier in de NAMEID/sub (UserID) en levert deze tevens als attribuut (eduPersonTargetedID)

Attributen
Beide leveren o.a. de volgende attributen

- eckId (ECKiD)
- eduPersonAffiliation, de rol (student, employee, staff)
- givenName (voornaam)
- sn (achternaam)
- ou (EF:klas/groep, SC:afdeling/team/faculteit)

Entree Federatie levert o.a. ook de volgende attributen:

- nlEduPersonRealId (userId)@realm)
- nlEduPersonProfileId (leerlingnummer@administratienummer.schooldomein.nl)
- nlEduPersonHomeOrganizationId (BRIN)
- nlEduPersonHomeOrganization (de naam van de school)
- nlEduPersonHomeOrganizationBranchId (Vestigingsnummer BRIN6)

SURFconext levert o.a. ook de volgende attributen:

- cn (volledige naam)
- displayName
- eduPersonPrincipalName(uid@schacHomeOrganization)
- eduPersonScopedAffiliation, de rol vanuit school (rol@schacHomeOrganization)
- schacHomeOrganization (de naam van de school)
- eduID (het eduID specifiek voor de dienst, alleen beschikbaar als eduID als login is gebruikt)

Schema's
Er worden niet alleen verschillende attributen geleverd ook worden er (voor dezelfde attributen) verschillende schema's (definitiestandaarden) gebruikt.

- Beide gebruiken attributen uit LDAP standaard
- Entree gebruikt verder vooral nlEduPerson
- SURFconext gebruikt vooral eduPerson[2] en Schac[3] (internationale schema's)

[2] eduPerson 2020-01 - Standards-and-Specs - REFEDS wiki
[3] SCHAC Releases - Standards-and-Specs - REFEDS wiki

Autorisaties
De autorisaties worden over het algemeen door de diensten zelf bepaald. Dit kan zijn op basis van een identifier, attribuut of een combinatie. SURFconext biedt een optie om dit bij de federatie te beleggen. De school kan zelf autorisatie regels aanmaken voor een dienst. Zie https://wiki.surfnet.nl/display/surfconextdev/Autorisatieregels.

Diensten die gegevens vanuit Entree Federatie gebruiken autoriseren bijvoorbeeld op de volgende gegevens:

- Identifiers: uid, nlEduPersonRealId, eckid, nlEduPersonProfileId
- eduPersonAffiliation; rol
- Organisatie of opleiding specifiek: nlEduPersonHomeOrganization(Id), nlEduPersonProfile, nlEduPersonDepartment, nlEduPersonUnit, ou, nlEduPersonCohort, ocwLTRegistratiecode, ocwLTLeerjaar, nlEduPersonHomeOrganizationBranchId

Diensten die gegevens vanuit SURFconext gebruiken autoriseren bijvoorbeeld op de volgende gegevens:

- Identifiers: uid, eduPersonTargetedID (gegenereerde nameID of sub), eduPersonPrincipalName (uid@instelling), eckid, ORCID, eduID
- eduPersonAffiliation; rol
- eduPersonEntitlement; autorisatie, wordt gezet door de IDP
- isMemberOf; groeplidmaatschap uit SURFconext Teams
- Organisatie of opleiding specifiek: schacHomeOrganization, ou

Een extra interessant attribuut dat SURFconext levert is het eduID. Deze targeted identifier wordt alleen geleverd als eduID als login is gebruikt. Het is niet helemaal zeker of ook geldt dat de gegevens vanuit de school (IdP) ook enkel geleverd worden na inloggen bij school (of als er al een sessie loopt). Vanuit de dienstaanbieder lijkt het wenselijk altijd dezelfde identifier/attribuut geleverd te krijgen en dat bijvoorbeeld enkel het betrouwbaarheidsniveau verandert als de dienst dat vereist.

Over het algemeen kan gesteld worden dat er wel ruimte is voor harmonisatie. Ook vragen we ons af of aantal attributen nog wel gebruikt worden. Er wordt besloten om in een volgende stap de attributen in te delen naar het doel waarvoor ze gebruikt worden. Een volgende stap kan dan zijn of die gegevens ook daadwerkelijk in het betreffende doel gebruikt worden (nog noodzakelijk zijn). Voor een aantal attributen zijn de doelen al gedefinieerd doordat het gebruikte schema hier bijvoorbeeld al een uitspraak over doet. Voorlopig onderkennen we de volgende doelen:

- Identificatie/authenticatie
- Autorisatie
- Business attributen (proces/dienst specifiek)
- Display attributen (specials, zoals casus achternaam)

Om dit verder uit te werken nemen we de volgende twee actiepunten op:

1. Uitwerken welke doelen we willen onderkennen voor identifiers en attributen en deze hieraan koppelen (actiepunt 12, Peter)
2. Nagaan welke doelen er nu in een ARP opgenomen zijn (actiepunt 13, Dirk)

UC2 – Confederatie SURFconext -> Entree Federatie

Momenteel zijn de federaties al gekoppeld. Het gaat echter alleen om de richting vanuit SURFconext scholen naar diensten van Entree Federatie. Op deze manier kunnen scholen

met een SURFconext koppeling (met name mbo) ook gebruik maken van de op Entree Federatie aangesloten diensten zonder dat de IdP/Authenticatiedienst van de school aan Entree Federatie gekoppeld hoeft te zijn. Om dit mogelijk te maken worden de identifiers/attributen van SURFconext vertaald naar de gegevens die Entree Federatie aan dienstaanbieders levert.

4. Notitie ROSA scan architectuurkaders

Als onderdeel van actiepunt #8 is er een begin gemaakt met het definiëren van architectuurkaders voor de ROSA scan. In de presentatie worden uitgangspunten en de kaders van een Digital identity trust framework toegelicht.

Uitgangspunten

Bij het uitgangspunt rond de te gebruiken bronnen wordt gevraagd waarom dit beperkt is tot bijvoorbeeld 'Visie digitale identiteit' van BZK. Er wordt aangegeven dat we de afgelopen tijd al vele documenten besproken hebben. We zullen zeker niets uitsluiten, maar willen nu een werkbaar vertrekpunt hebben. Daarbij speelt tevens dat er vanuit OCW terugkoppeling gevraagd wordt over de visie van BZK. Een aantal inhoudelijke aspecten van die visie zijn ook opgenomen in de presentatie zodat we kunnen toetsen of wat wij binnen de onderwijssector willen aansluit op de visie. De leden worden verder vooral opgeroepen om interessante stukken of projecten aan de werkgroep te blijven melden. Er is veel beweging rond het thema IAA en we willen op de hoogte blijven, maar moeten bij het ontwikkelen van kaders hier niet op vastlopen.

Bij het uitgangspunt dat we kaders definiëren voor de hele onderwijssector ontstaat wat discussie. Wat is precies de onderwijssector en moeten we ook niet Leven Lang Ontwikkelen binnen de scope opnemen? Er wordt aangegeven dat we ook dit als een vertrekpunt zien en dat de scope niet formeel vastgesteld is. In essentie willen we kaders binnen de ROSA/ Edustandaard definiëren waar we ook enigszins grip hebben op het naleven ervan. Het gaat er dan concreet om van welke projecten we verwachten dat er een ROSA scan wordt aangevraagd. Dit kan vanuit de projecten zelf zijn of bijvoorbeeld leden van de Architectuurraad. We stellen (voorlopig) dat dit projecten binnen het onderwijs zijn (primaire of secundaire proces) waarvoor binnen het thema IAA iets ontwikkeld wordt. We denken hierbij bijvoorbeeld aan eduID, EDUmij of doorontwikkeling van Entree Federatie. Een ander aspect zijn de (externe) oplossingsrichtingen die we mogelijk binnen de onderwijssector willen hergebruiken. Het klopt dus dat we zeker niet noodzakelijk alleen naar oplossingen binnen de onderwijssector kijken. Zo moeten we ook een generieke oplossing voor het machtigen van medewerkers (denk bijvoorbeeld aan eHerkenning) kunnen toetsen. We hebben dus een algemeen beeld van de scope, maar weten dat we dit op een later moment beter zullen moeten formuleren.

Digital identity trust framework

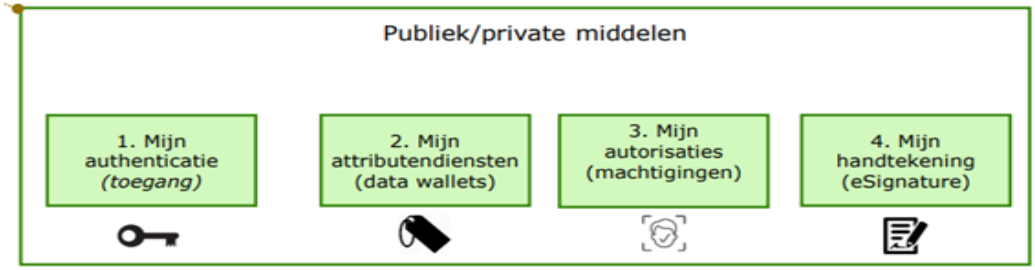
We ontwikkelen kaders voor het uitvoeren van een ROSA scan voor het thema IAA. We definiëren dus geen afsprakenstelsel, maar bij het opstellen van de kaders leek het verstandig om toch ook van een trust framework te spreken. Dit geeft de mogelijkheid om de rollen beter te kunnen duiden. In de kern gaat het namelijk om een dienst en een dienstafnemer, maar binnen het stelsel zijn er verschillende rollen/functies/voorzieningen etc. die het toegangsproces faciliteren. Voor zowel de rollen als de generieke functies wordt aangesloten bij de visie van BZK.

<u>Rollen</u>

De rollen zijn vergelijkbaar met het generieke use case model dat we in het use case document hebben opgenomen. Wel onderkennen we dat de visie van BZK afwijkende begrippen gebruikt. Wij volgen momenteel de NORA op dit vlak. Zowel de NORA als GO

zijn echter gebruikt voor de ontwikkeling van de visie, maar we verwachten dat uiteindelijk dezelfde begrippen toegepast gaan worden.

Generieke functies
Binnen het digital identity trust framework worden vier functies onderscheiden, dit zijn Identificatie & Authenticatie (Mijn authenticatie), Gegevensuitwisseling (Mijn Attributendiensten), Machtigen en Vertegenwoordiging (Mijn Autorisaties) en digitaal ondertekenen (Mijn Handtekening). Met het apart benoemen van 'Mijn Authenticatie' en 'Mijn Attributendiensten' wordt aangegeven dat er een logische scheiding is tussen toegang en het uitwisselen van (persoons)gegevens.



De komende periode worden de ROSA scan kaders die we binnen het Digital identity trust framework onderkennen verder ontwikkeld en zullen regelmatig terugkomen op de agenda.

5. Rondvraag & afsluiting

Het volgende overleg is op 24 juni van 1500 tot 1700 uur. Op de agenda staan dan de volgende onderwerpen:

- Mededelingen en opening
- Verslag 20 mei 2021 & acties
- Gemeenschappelijke Overheidsarchitectuur (indien versie beschikbaar)
- Doorontwikkelen ROSA scan architectuurkaders

6. 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	Open		Paul (en Peter)
7	Uitwerken use cases irt federaties	Afgehandeld		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
9	Wat willen we de informatiekamer meegeven mbt de Visie op digitale identiteit van BZK	Afgehandeld		werkgroep
10	Wat kunnen wij eventueel van de BZK visie overnemen (in verschillende referentie architecturen waarin het thema toegang is opgenomen)	Afgehandeld		werkgroep
11	Nieuwe versie GO I&A-Machtigen op Drive plaatsen	Open		Frits

12	Uitwerken welke doelen we willen onderkennen voor identifiers en attributen en deze hieraan koppelen	Open		Peter
13	Nagaan welke doelen er nu in een ARP opgenomen zijn	Open		Dirk

BES = Bureau Edustandaard
Grijs = afgehandeld of vervallen