Edukoppeling

Discussiestuk OAuth/SaaS-profiel

Edustandaard

Datum: september 2022

Inhoudsopgave

1. Documenthistorie

Versie	Auteur	Datum	Opmerking
0.1	E. Reinhoud	12 september 2022	Initiële versie

2. Inleiding

2.1. Aanleiding

Edukoppeling is een belangrijke bouwsteen in de ketenreferentiearchitectuur ROSA[1]. Het functionele toepassingsgebied van de Edukoppeling SaaS-profielen betreft de uitwisseling van persoonsgegevens die door SaaS-leveranciers (verwerker) namens een onderwijsinstelling (eindorganisatie) worden uitgevoerd. De SaaS-profielen bevatten voorschriften voor beveiliging en het kunnen routeren (o.b.v. een routeringskenmerk) naar een bepaalde tenant (een bepaalde administratie van een onderwijsinstelling).

Voor hun koppelingen in de ECK-keten heeft Topicus een OAuth client credentials profiel in gebruik genomen dat ook als onderdeel van het nieuwe SEM Ecosysteem is ingebracht. Dit profiel wordt toegepast bij uitwisselingen waarbij Topicus als bronhouder van persoonsgegevens namens een onderwijsinstelling deze gegevens verstrekt aan een derde partij. In de ECK-keten zijn meerdere partijen die als bronhouder persoonsgegevens kunnen delen met derde partijen en dus is de verwachting dat meerdere partijen een dergelijk OAuth-profiel willen gaan gebruiken. Het risico hierbij is dat er bij de inrichting verschillende keuzes worden gemaakt. Er wordt nu aan de Edukoppeling werkgroep gevraagd om tot een gestandaardiseerd OAuth-profiel te komen die breed inzetbaar is binnen het onderwijs in de SaaS-context.

We pakken de ontwikkeling van het Edukoppeling OAuth-profiel op zonder vooraf al een duidelijke voorkeur te hebben over de nog te maken keuzes. Deze keuzes zijn in principe aan de werkgroep, maar we hebben wel te maken met de kaders van de ROSA. Daarnaast zijn er verschillende ontwikkelingen die het definiëren van een OAuth standaard complex maken. Met dit document hopen we de complexiteit te beperken door overzicht te bieden. In dit document willen we de aandachtspunten kaderen en de besluiten herleidbaar maken. Op basis van deze besluiten zal het uiteindelijke OAuth-profiel opgesteld worden. Het doel is dus om tot een profiel te komen wat interoperabel en breed inzetbaar is binnen het onderwijs. Het moet leiden tot een onderwijsspecifieke standaard voor M2M uitwisselingen waarbij er speciaal aandacht is voor de SaaS-context[2].

2.2. Relatie met bestaande profielen en OSR

Momenteel is er al een Edukoppeling REST/SaaS-profiel, maar net als het WUS/SaaS-profiel gaat het hierbij enkel om standaardisatie van routering van het “bericht”. Het profiel bestaat met name uit afspraken rond het routeringskenmerk en de beveiligde mTLS verbinding. Bij het REST/SaaS-profiel wordt hierbij gebruik gemaakt van een query string waarbij het om een point-to-point koppeling gaat en de afspraak geldt dat het to-kenmerk en from-kenmerk in de response de inverse zijn van het request.

In de Edukoppeling Architectuur wordt ook een Onderwijs serviceregister (OSR) onderkend. In OSR kunnen scholen en onderwijsinstellingen op één centrale plek vastleggen welke systemen namens de school berichten mogen uitwisselen voor verschillende diensten. Ook wel mandateren genoemd. De leveranciers van de systemen leggen vervolgens de

[1] https://www.wikixl.nl/wiki/rosa/index.php/Hoofdpagina
[2] Zie toelichting **Fout! Verwijzingsbron niet gevonden.**

technische afleveradressen vast in het OSR zodat berichten voor de school op de juiste plek kunnen worden afgeleverd.

Een OAuth Authorization Server kan een vergelijkbare functie hebben als het OSR heeft rond mandaten. Partijen kunnen bij het OSR het mandaat verifiëren via een API. Bij Oauth wordt de autorisatie in de uitwisseling meegenomen in de vorm van een Access Token[3]. OAuth geeft geen invulling aan de SaaS-context zoals we die nu binnen Edukoppeling kennen. Hiervoor zijn dus aanvullende kaders nodig.

2.3. Doel en status van dit document

Dit is de eerste versie van dit document. Het zal geen onderdeel vormen van de uiteindelijke Edukoppeling afspraak, maar dient alleen voor transparantie van het proces door het inzichtelijk maken van relevante informatie en het traceerbaar maken van de verschillende te maken keuzes.

Deze initiële versie is een eerste aanzet met de benodigde achtergrondinformatie en een voorstel rond een aantal relevante overwegingen. Het is aan de werkgroep om overwegingen toe te voegen, wijzigen of verwijderen. Voordat een profiel opgesteld kan worden dienen de overwegingen en gemaakte keuzes vastgesteld te worden.

[3] Een Oauth profiel kan echter ook zogenaamde introspectie ondersteunen waarbij een Access Token (niet zelfbeschrijvend/vertrouwd) bij de OAuth Authorization Server geverifieerd kan worden.

3. Uitgangspunten

De uitgangspunten worden gevormd door de besluiten die we bij de overwegingen hebben gemaakt. Hieronder staan de belangrijkste uitgangspunten[4].

1. …

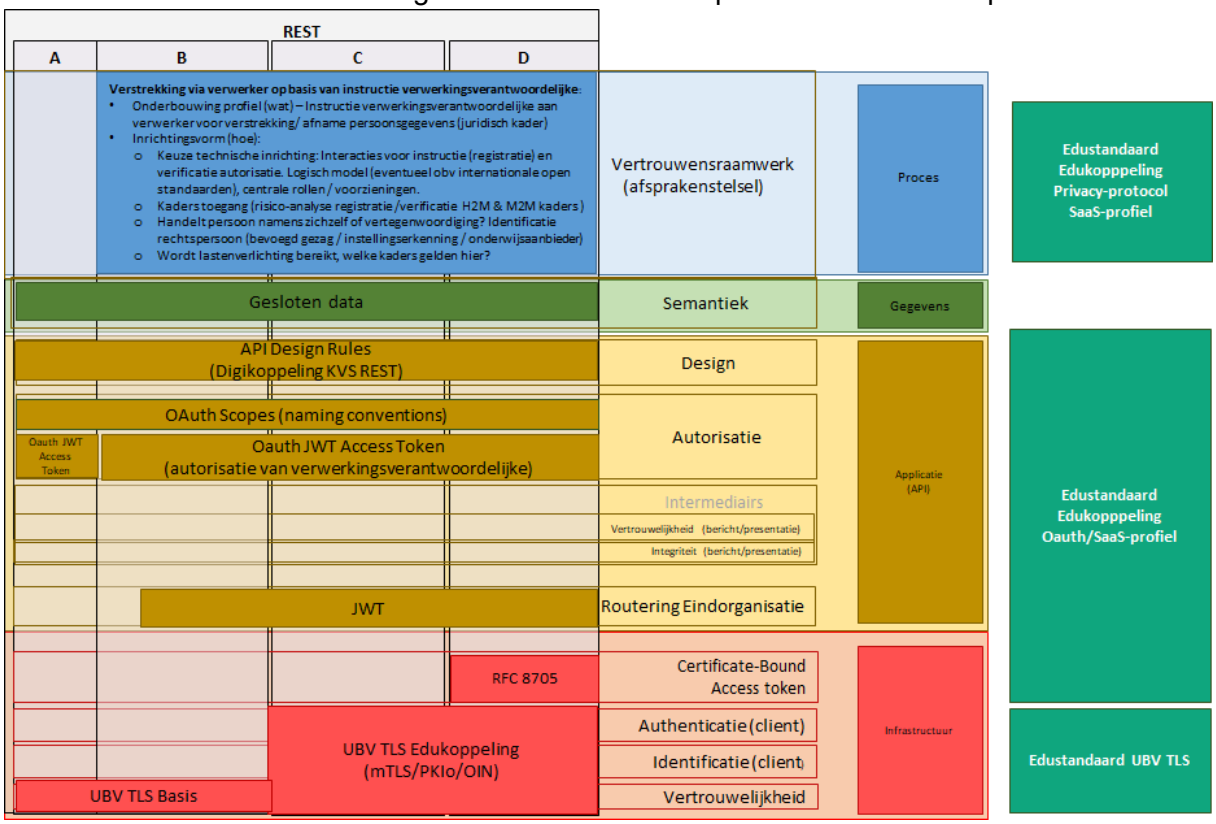
[4] In deze 0.1 versie zijn er nog geen besluiten genomen. Er zijn dus geen uitgangspunten.

4. Overwegingen

In dit hoofdstuk overwegingen opgenomen rond de te maken keuzes. De overwegingen zijn ingedeeld naar het Edukoppeling informatie-uitwisselingsmodel. Deze is zo opgebouwd dat de verschillende lagen ontkoppeld zijn, maar wel op elkaar aansluiten.

4.1. Opbouw OAuth-profiel

De combinatie van een aantal “hoog over” keuzes vormen een belangrijk vertrekpunt voor het OAuth-profiel. In Figuur 1 worden de verschillende lagen schematisch weergegeven. De keuzes over de verschillende lagen vormen het vertrekpunt voor het OAuth-profiel.



Figuur 1 - Edukoppeling Informatie-uitwisselingsmodel

In de kolom ‘REST’ zijn een viertal kolommen (‘A’, ‘B’, ‘C’ en ‘D’) opgenomen. Elke kolom is een samenstelling van keuzes in de verschillende lagen. Er zijn in feite veel meer keuzes in dit document opgenomen, maar op basis van deze vier combinaties denken we een duidelijk vertrekpunt te kunnen definiëren. Het helpt ons om in een vroeg stadium een gedeeld beeld te hebben waar het profiel wel en niet over gaat. Verder hoeft op termijn het één de ander niet uit te sluiten, maar het is goed om in deze fase het over één profiel te hebben.

A. Edukoppeling OAuth-profiel[5]
   a. Geen proceslaag, de SaaS-context wordt NIET onderkend
   b. Toepassing API Design Rules
   c. Geen OAuth Access Token als autorisatie van een verwerkingsverantwoordelijke aan een verwerker voor verstrekking van persoonsgegevens
   d. Geen JWT routeringstoken
   e. UBV TLS basis, TLS en geen PKIo /OIN

B. Edukoppeling OAuth/SaaS-profiel
   a. Proceslaag met registratie autorisatie
   b. Toepassing API Design Rules
   c. OAuth Access Token vertegenwoordigd autorisatie van een verwerkingsverantwoordelijke aan een verwerker voor verstrekking van persoonsgegevens
   d. JWT routeringstoken
   e. UBV TLS basisprofiel, TLS en geen PKIo /OIN

C. Edukoppeling OAuth/SaaS-profiel
   a. Proceslaag met registratie autorisatie
   b. Toepassing API Design Rules
   c. OAuth Access Token vertegenwoordigd autorisatie van een verwerkingsverantwoordelijke aan een verwerker voor verstrekking van persoonsgegevens
   d. JWT routeringstoken
   e. UBV TLS Edukoppeling profiel, mTLS & PKIo & OIN

D. Edukoppeling OAuth/SaaS-profiel
   a. Proceslaag met registratie autorisatie
   b. Toepassing API Design Rules
   c. OAuth Access Token vertegenwoordigd autorisatie van een verwerkingsverantwoordelijke aan een verwerker voor verstrekking van persoonsgegevens
   d. JWT routeringstoken
   e. UBV TLS Edukoppeling profiel, mTLS & PKIo & OIN
   f. Binding van Access Token met mTLS certificaat (RFC8705)

Opbouw OAuth-profiel

Voorstel: Kolom ‘D’ is de gewenste samenstelling om tot een OAuth-profiel te komen. We hebben het dan dus over een OAuth/SaaS-profiel

Toelichting: We ontwikkelen een OAuth/SaaS-profiel waarmee de ‘SaaS’-context ondersteund wordt. Hierbij passen we het UBV TLS Edukoppeling profiel toe en sluiten hiermee aan op de infrastructuurlaag van de bestaande SaaS-profielen. Dit biedt ook de

[5] Deze variant is opgenomen omdat we in de nieuw op te stellen architectuur de ruimte bieden aan profielen op basis van het UBV TLS basisprofiel en profielen die functioneel buiten de SaaS-context vallen. De internationale, nationale standaard en vrijwel alle OAuth implementaties kennen de SaaS-context niet.

mogelijkheid om client authenticatie en Acces Token binding uit te voeren op basis van het mTLS certificaat (RFC8705).

4.1. Proceslaag

Op basis van de keuze voor een OAuth/SaaS-profiel stellen we dat ook de proceslaag relevant wordt. De Edukoppeling SaaS-profielen kunnen we zien als privacy bevorderende maatregelen om datalekken te voorkomen. De uitwisseling van persoonsgegevens kan pas plaatsvinden als er gecontroleerd is dat de partijen aan een aantal voorschriften voldaan hebben. In de proceslaag gaat het om voorschriften rond interacties tussen de verschillende rollen.

Voorstel P1: De proceslaag wordt onderdeel van de normatieve voorschriften voor Edukoppeling SaaS-profielen.

Toelichting: De Edukoppeling-standaard beperkt zich nu tot de applicatie- en infrastructuurlaag waarmee op transport- en berichtbeveiliging en interoperabiliteit wordt bereikt. Verder wordt voor de SaaS-context de functie ondersteund om het bericht te kunnen routeren van een verwerker naar een bepaalde eindorganisatie. We hebben al eerder in de werkgroep geconstateerd dat de huidige lagen eigenlijk niet voldoende zijn. De interacties rond registratie en verificatie van de mandatering moeten onderdeel zijn van de standaard. Er ontbreekt nu een normatief document dat het verplicht gebruik en de voorschriften van de proceslaag beschrijft.

De kaders voor de proceslaag moeten uitgewerkt worden en komen in een apart document. Deze worden gebruikt naast de profielvoorschriften (REST/SaaS-profiel, WUS/SaaS-profiel en OAuth/SaaS-profiel) en het I&A document.

In hoeverre er overlap is in de kaders voor OSR en OAuth zal bij uitwerking blijken.

Voorstel P2: **De kaders voor de proceslaag worden in een SaaS privacy-protocol beschreven.**

Toelichting: Binnen de Edustandaard Architectuuraanpak Toegang[6] worden een aantal concepten gebruikt die we ook binnen Edukoppeling willen toepassen. De Architectuuraanpak Toegang bevat een aanpak om verschillende inrichtingsvormen voor het delen van (persoons)gegevens te analyseren. Het kan hierbij gaan om een digitale identiteit die voor toegang tot een dienst nodig is, maar er wordt ook gekeken naar andere concepten zoals SSI. Ook het verstrekken van persoonsgegevens door een verwerker wordt onderkend (zoals in de context van Edukoppeling).
De inrichtingsvormen worden opgedeeld door een modulaire opbouw te onderkennen. In de basis gaat het om een aantal generieke functies die relevant zijn, zoals identificatie, authenticatie en autorisatie (IAA), maar ook functies die de privacy bevorderen. Deze generieke functies kunnen worden toegepast in verschillende contexten (federatieve

[6] https://www.edustandaard.nl/standaard_afspraken/architectuuraanpak-toegang/

toegang, SSI, verstrekking via verwerker…) en worden vervolgens op conceptueel niveau beschreven in zogenaamde toepassingspatronen[7].

De Edukoppeling-standaard kunnen we dan ook als een toepassingspatroon beschouwen. Het kenmerk van het Edukoppeling toepassingspatroon is de uitwisseling van (persoons)gegevens waarbij ten minste één van de partijen een verwerker is die namens een eindorganisatie persoonsgegevens verwerkt (SaaS-context). In het toepassingspatroon worden de procestappen en functies beschreven die moeten zijn uitgevoerd voordat deze uitwisseling mag plaatsvinden. Dit is wat we ook met de ontwikkeling van dit OAuth/SaaS-profiel beogen.

De concrete aansluiting op de Architectuuraanpak Toegang komt tot stand met het toepassen van een zogenaamd privacy-protocol. Het privacy-protocol vormt de kern binnen een toepassingspatroon en beschrijft de privacy bevorderende maatregelen. Voor Edukoppeling kunnen we een SaaS privacy-protocol opstellen met hierin de interacties en de kaders die gelden (zie de proceslaag in Figuur 1). Er wordt een beschrijving gegeven wat er met het profiel bereikt wordt en hoe hier invulling aan wordt gegeven. Wat er bereikt wordt heeft een relatie met het juridisch kader.

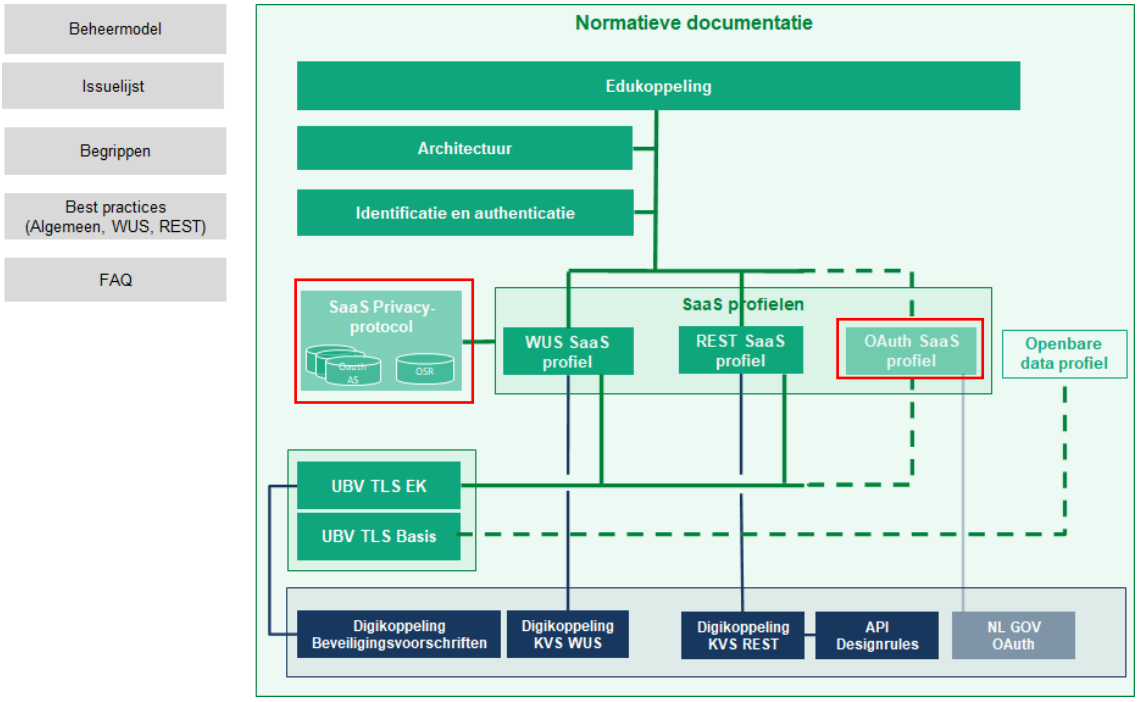
Waar we het SaaS privacy-protocol in Edukoppeling documentatie borgen staat nu nog open. De inhoud kan in de architectuur opgenomen worden, maar we verwachten wel dat het dan een groot deel van de architectuur zal worden. Daarnaast gaat het ook om een juridisch kader en ook de inrichtingsvorm(en) en bijbehorende interacties. Dit zit op het grensvlak van de architectuur. Verder krijgt de Architectuur zoals afgesproken een breder perspectief met ook andere profielen en gebruik van UBV TLS basis. De SaaS-context staat dus niet meer centraal.

Doordat we nu niet meer alleen normatief de logistieke laag (bericht en transport) voorschrijven, maar ook de kaders voor het proces (rollen en interacties) kunnen we stellen dat nu meer sprake is van een afsprakenstelsel. Het SaaS privacy-protocol kan gebruikt worden binnen een afsprakenstelsel. Het geeft het juridisch kader weer (WAT) en de inrichtingsvorm (HOE) en verantwoordelijkheid van de verschillen rollen hierbinnen. Bij de ontwikkeling van een ketenafspraak kan hier naar gerefereerd worden of deze elementen kunnen overgenomen worden.

Er wordt nu aangenomen dat er één SaaS privacy-protocol is die in combinatie met alle SaaS-profielen gebruikt moet worden. Bij de uitwerking kan het echter zijn dat we tot de conclusie komen dat het beter is om voor de bestaande REST en WUS SaaS-profielen en het gebruik van het OSR een apart privacy-protocol op te stellen. Dit omdat de het OSR een centraal component is en eigen interacties kent.
Bij OAuth hebben we (voorlopig) waarschijnlijk te maken met meerder lokale Authorization servers. In **Fout! Verwijzingsbron niet gevonden.** wordt het normatieve SaaS privacy-protocol schematisch binnen Edukoppeling weergegeven.

---

[7] Een ander voorbeeld van een toepassingspatroon is het SSI concept waar de betrokkene zelf regie voert over de (persoons)gegevens. De Architectuuraanpak Toegang en de toepassingspatronen zijn nog in ontwikkeling.

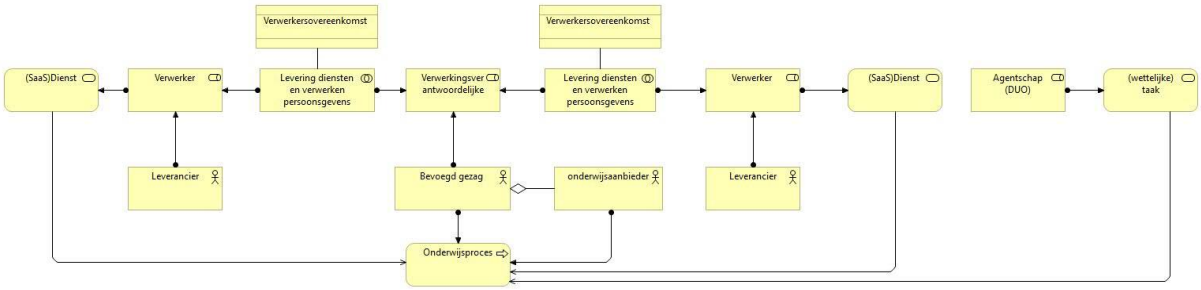


Figuur 2 – Positionering van Privacy protocol en OAuth profiel binnen Edukoppeling

Voorstel P3: **Onderdeel van het SaaS privacy-protocol is het juridisch kader.**

Toelichting: Een belangrijk onderdeel binnen het privacy-protocol zijn de kaders van de AVG. Belangrijke actoren binnen de AVG zijn de (gegevens)betrokkene, de verwerkingsverantwoordelijke en de verwerker. De betrokkene[8] is de natuurlijke persoon op wie de persoonsgegevens betrekking hebben. De verwerkingsverantwoordelijke is degene het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. De verwerker is de partij die ten behoeve van/in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. Het is dus afhankelijk van de situatie wie de verwerkingsverantwoordelijke is. Binnen de context van de SaaS-profielen betreft het een onderwijsaanbieder (bevoegd gezag) die een dienst afneemt van een (SaaS) leverancier die aan de onderwijsprocessen ondersteuning biedt. Het bevoegd gezag is dus de verwerkingsverantwoordelijke en de leverancier verwerker (zie Figuur 3).

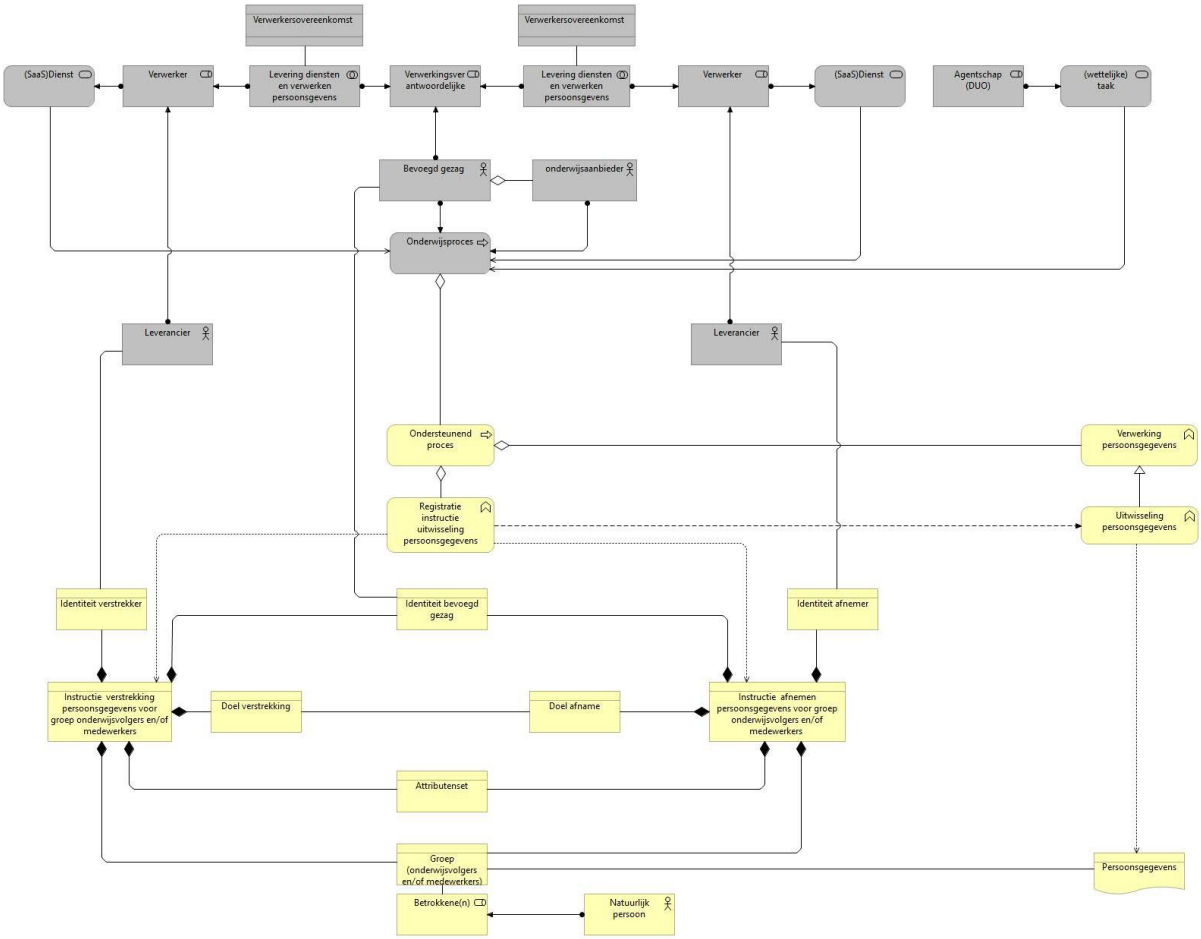
[8] De betrokkene betreft over het algemeen de onderwijsvolger die niet handelingsbevoegd (po, vo en mbo sector) is. De betrokkene kan echter ook een medewerker van een onderwijsinstelling betreffen. De onderwijsaanbieder (vallend onder een eindverantwoordelijk bevoegd gezag) is verantwoordelijk om opvolging te geven aan de rechten van de betrokkene en valt buiten de scope van het SaaS-profiel.



Figuur 3 - Juridisch kader verwerker

Voor een bepaald onderwijsproces kan het noodzakelijk zijn dat twee verwerkers namens de verwerkingsverantwoordelijke persoonsgegevens moeten uitwisselen[9]. Het bevoegd gezag heeft dan met beide[10] verwerkers (de één als (gegevens)verstrekker de ander als (gegevens)afnemer) een verwerkersovereenkomst. Verder heeft het bevoegd gezag beide verwerkers vooraf aan de uitwisseling geautoriseerd om voor het betreffende doel persoonsgegevens uit te wisselen. Deze autorisatie heeft dus een relatie met een verwerkersovereenkomst, maar er is in principe een aparte instructie[11] voor de verstrekking. In de context van de AVG hebben de leveranciers (verwerkers) beide de instructie van het bevoegd gezag (verwerkingsverantwoordelijke) gekregen om voor een bepaald doel een bepaalde set persoonsgegevens[12] (van betrokkenen) uit te wisselen. De autorisatie voor de verstrekking vormt de kern van de SaaS-profielen en wordt (digitale registratie) wordt onderdeel van de interacties in de proceslaag[13].

[9] Onder verwerken vallen alle handelingen die een organisatie kan uitvoeren met persoonsgegevens, van verzamelen tot en met vernietigen, maar ook het verstrekken aan een andere partij.
[10] Het kan ook zijn dat één van beide partijen de gegevens verwerkt zonder instructie van de verwerkingsverantwoordelijke (bijvoorbeeld DUO in de rol van een agentschap met een wettelijke taak).
[11] In de verwerkersovereenkomst staan over het algemeen niet ook alle verstrekkingen of afname van een derde partij.
[12] Van een bepaalde groep (onderwijsvolgers en/of medewerkers) een bepaalde set attributen.
[13] De verwerkersovereenkomst is in principe buiten scope.



Figuur 4 - Juridisch kader registratie autorisaties voor verwerkers (de één voor verstrekking, de ander voor afname van persoonsgegevens)

Tot nu toe hebben we het binnen Edukoppeling o.a. over SaaS-leveranciers, SaaS-diensten, SaaS-profielen en eindorganisaties. Onderdeel van de ROSA herziening is om ook naar de Edukoppeling begrippenlijst[14] te kijken en deze op te nemen in het ROSA Begrippenmodel. Een betere aansluiting op het juridisch kader kan ook bijdragen aan begrippen die beter passen.

Voorstel P4: **Onderdeel van het SaaS privacy-protocol zijn de interacties.**

Toelichting: Een ander belangrijk onderdeel binnen het privacy-protocol zijn de interacties (H2M en M2M) en de kaders die hierbij gelden. Deze worden deels bepaald door bestaande kaders binnen Edukoppeling en deels aangevuld. Met de Architectuuraanpak Toegang en

[14] Het nieuwe ROSA begrippenkader wordt in september met de werkgroep besproken

ROSA referentie-architectuur[15] nemen we binnen het privacy-protocol aanvullende kaders op.

Zo zullen er bij de registratie van de autorisatie[16] voor verstrekking en afname (H2M interacties) toegangseisen worden gesteld. De digitale identiteit van de onderwijsmedewerker die deze handeling uitvoert moet van een bepaald betrouwbaarheidsniveau[17] zijn. Welk betrouwbaarheidsniveau geldt moet de verwerker die de autorisatie registreert bepalen op basis van een risicoanalyse. Er moet ook vastgesteld kunnen worden dat de medewerker bevoegd is om namens het bevoegd gezag te handelen (gemachtigd). De identiteit die de medewerker heeft gemachtigd moet herleidbaar zijn naar de entiteit in het juridisch kader, de verwerkingsverantwoordelijke. Deze is verantwoordelijk voor het geven van de instructie dat een verwerker persoonsgegevens mag delen met een derde. Deze herleidbaarheid wordt door RIO ondersteund.

Er zijn ook M2M interacties. Beide verwerkers moeten vooraf bij elkaar hebben vastgesteld dat de autorisatie is gegeven. Deze verificaties zijn onderdeel van interacties in het privacy-protocol waarvoor ook kaders rond toegang worden opgenomen. Het toepassen van OAuth zorgt ervoor dat de gegevens (gebruik API) alleen uitgewisseld kunnen worden als de verstrekker de afnemer een valide access token heeft geleverd. Het access token is dus een extra technische maatregel[18] bovenop de verificatie van de autorisatie.

Voorstel P5: **Het functionele toepassingsgebied van het OAuth/SaaS-profiel betreft een RESTful M2M gegevensuitwisseling via een beveiligde point-to-point verbinding <u>waarbij tenminste één partij dit in opdracht doet van een verwerkingsverantwoordelijke.</u>**

Toelichting: In de context van dit OAuth profiel betreft het uitwisselingen van persoonsgegevens waar het bevoegd gezag de verwerkingsverantwoordelijke is en dus het doel en het middel vaststelt voor verwerking (dus ook verstrekking). De gegevens kunnen op basis van de afspraken binnen dit profiel gerouteerd worden tussen een verwerker en eindorganisatie. Dit laatste is geen verplichting indien de eindorganisatie ook de rol van verwerker heeft.

4.2. Applicatielaag

[15] De ROSA wordt momenteel herzien op verschillende punten. Een aantal kaders zullen dus nog in ontwikkeling zijn, maar verwachten rond einde 2022 een redelijke stabiele ROSA te hebben.
[16] Wordt in de context van OSR nu ook wel mandaat genoemd.
[17] Mate waarin vertrouwen kan worden gesteld in een identificatiemiddel, gebaseerd op de mate van zekerheid waarmee attributen, identiteiten, identificatiemiddelen en/of bevoegdheden zijn vastgesteld.
[18] Op technisch niveau wordt de uitwisseling geblokkeerd als de verstrekker de bevoegdheid van afnemer niet heeft kunnen vaststellen.

Voorstel A1: **Het NL GOV OAuth profiel vormt de basis voor de applicatielaag.**

Toelichting: Er moet een keuze worden gemaakt welke OAuth standaard we als basis gebruiken, Er is de internationale open standaard zelf, het iGOV profiel en het NL GOV OAuth profiel. Deze ondersteunt nu alleen code grant profiel (zie bijlage A). Wel is men het client credentials profiel aan het ontwikkelen wat deels een afgeleide is van het bestaande code grant profiel.

Voorstel A2: **We gebruiken het OAuth client credentials profiel als basis voor de interacties in de applicatlelaag.**

Toelichting: In de use case past ook het code grant profiel als de onderwijsaanbieder als resource owner wordt beschouwd.

Voorstel A3: **We gaan er (nu nog) vanuit dat de OAuth Authorization Server door meerdere partijen geïmplementeerd kan worden.**

Toelichting: We gaan in eerste instantie uit van een profiel met een decentrale Authorization Server. Dit betekent dat zowel de registratie als de uitgifte van het Access Token door authorization servers wordt uitgevoerd die in hetzelfde (netwerk/beveiligings)domein staan als de resource server(s).

Beveiliging eigen API's (via Resource Server). De AS en RS bevinden zich dus in hetzelfde (beveiligings)domein.

4.3. Infrastructuurlaag

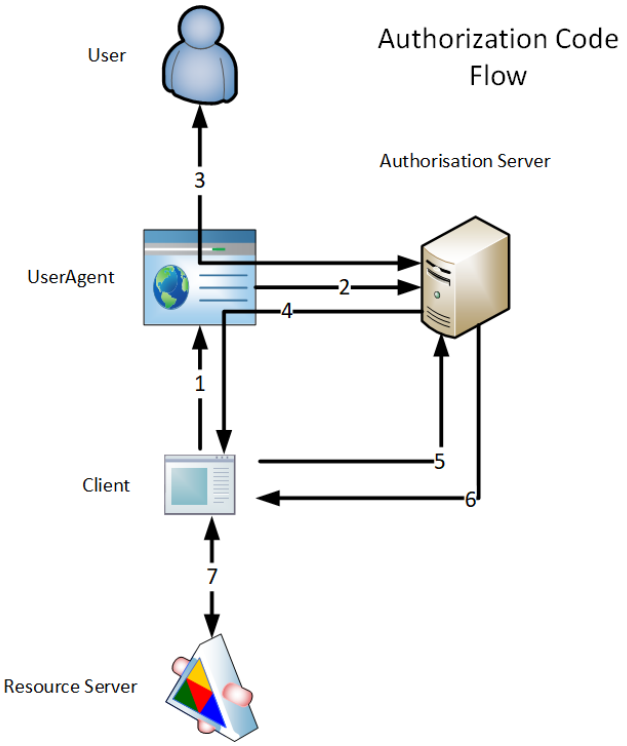
Op dit niveau verwachten we geen impact. We passen het UBV TLS basis of UBV TLS Edukoppeling profiel toe.

5. Bijlage A: OAuth 2.0 profielen

5.1. OAuth 2.0 - Code Grant profile

Binnen de OAuth-standaard worden 4 rollen onderkend, de User (Resource Owner / RO), de Resource Server (RS), de Client en de Authorization Server (AS). OAuth introduceert een expliciete autorisatielaag tussen de RO en Client. Het gaat hierbij om zogenaamde gedelegeerde autorisatie. De RO bepaalt welke van de gegevens aan de client beschikbaar worden gesteld. Deze gegevens worden via beschermde API's ontsloten die zijn gehost op een bepaalde RS. De RO registreert hiervoor bevoegdheden bij de AS en de client kan via een door de AS geleverd toegangstoken toegang krijgen tot de gegevens van de API die binnen de betreffende bevoegdheden vallen. De RO vertrouwt de client dus voldoende dat deze over betreffende gegevens komt te beschikken.

De OAuth-standaard ondersteund verschillende profielen. Het hierboven beschreven scenario komt overeen met het zogenaamde Code Grant profiel[19]. De interacties waar dit profiel uit bestaat wordt weergegeven in figuur 1.



Figuur 5 OAuth Code Grant profile

5.1.1. Client typen

OAuth definieert twee typen clients. De indeling is gebaseerd op de mate waarin een betrouwbare authenticatie door de autorisatieserver mogelijk is. Het betreft hierbij in hoeverre ze in staat zijn hun credentials vertrouwelijkheid te bewaren. De OAuth-specificatie onderkent op basis hiervan Confidential clients en Public clients.

[19] Zie voor meer details RFC 6749 - The OAuth 2.0 Authorization Framework (ietf.org)

- Confidential
  Clients capable of maintaining the confidentiality of their credentials (e.g., client implemented on a secure server with restricted access to the client credentials), or capable of secure client authentication using other means.

- Public
  Clients incapable of maintaining the confidentiality of their credentials (e.g., clients executing on the device used by the resource owner, such as an installed native application or a web browser-based application), and incapable of secure client authentication via any other means.

De OAuth-specificatie onderkent verder verschillende client profiles die meer context geven bij een bepaald client type. De specificatie onderkent een web application, user-agent en een native application client profile.

- web application
  "*A web application is a confidential client running on a web server. Resource owners access the client via an HTML user interface rendered in a user-agent on the device used by the resource owner. The client credentials as well as any access token issued to the client are stored on the web server and are not exposed to or accessible by the resource owner."*

- user-agent-based application
  "*A user-agent-based application is a public client in which the client code is downloaded from a web server and executes within a user-agent (e.g., web browser) on the device used by the resource owner. Protocol data and credentials are easily accessible (and often visible) to the resource owner. Since such applications reside within the user-agent, they can make seamless use of the user-agent capabilities when requesting authorization."*

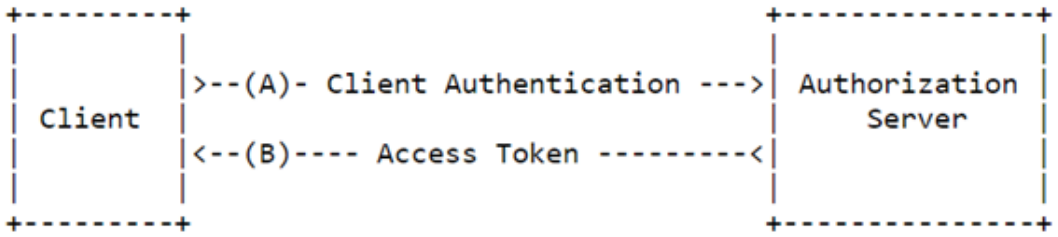
- native application
  "*A native application is a public client installed and executed on the device used by the resource owner. Protocol data and credentials are accessible to the resource owner. It is assumed that any client authentication credentials included in the application can be extracted. On the other hand, dynamically issued credentials such as access tokens or refresh tokens can receive an acceptable level of protection. At a minimum, these credentials are protected from hostile servers with which the application may interact. On some platforms, these credentials might be protected from other applications residing on the same device*."

5.2. OAuth 2.0 - Client credentials grant profile[20]

Een ander OAuth 2.0 profiel is het client credentials grant profiel. Dit is een profiel waarbij geen RO betrokken is. De client verkrijgt alleen een toegangstoken voor een resource van de autorisatieserver via zijn eigen client credentials, in tegenstelling tot het aanvragen van

[20] Zie voor meer details https://datatracker.ietf.org/doc/html/rfc6749

toegang namens een RO. In de context van OAuth zou gesteld kunnen worden dat de client zelf de RO is: er is geen delegatie. In dit geval is het dus niet helemaal duidelijk hoe bevoegdheden worden uitgedrukt, het kan bijvoorbeeld zijn dat bevoegdheden eerder (buiten de scope van OAuth) bij de autorisatieserver zijn geregistreerd. De interacties waar dit profiel uit bestaat wordt weergegeven in Figuur 6Figuur 6.



Figuur 6- OAuth Client credentials grant profile

5.2.1. Client typen

Het client credentials grant profiel is alleen van toepassing bij confidential clients (web application profile clients).

5.3. NL GOV Assurance profile for OAuth 2.0 v1.0[21]

Er is op basis van het OpenID iGOV[22] profiel een profiel opgesteld voor de Nederlandse overheid. Het NL GOV Assurance profile for OAuth 2.0 is opgenomen in de pas-toe-of-leg-uit lijst van Forum Standaardisatie[23]. Het legt bindende afspraken vast over het gebruik van de standaard OAuth 2.0 bij de Nederlandse overheid. In combinatie met onderliggende standaard OAuth 2.0 zorgt NL GOV Assurance profile for OAuth 2.0 ervoor dat de autorisatie van gebruikers van REST APIs van de overheid op een uniforme en eenduidige plaatsvindt. De use cases waar dit profiel kan worden toegepast komt overeen met Figuur 5 en is als volgt gedefinieerd:

> "*In this use case a (public/governmental) service is offered via an API. The service will be consumed by the User using a client, that can be any arbitrary, non-trusted application. For provisioning the service, the service provider requires an identifier of the User. The identifier of the User can be either an arbitrary (self-registered) identifier or a formal identifier (citizen number or other restricted, registered ID). Upon service provisioning, the service uses the identifier of the User for access control within the service.*"

De huidige vastgestelde versie (9 juni 2020) van het NL GOV Assurance profile for OAuth 2.0 bevat met name wijzigingen rond het iGOV Code Grant profiel waar het op gebaseerd is. Het direct access (client credentials grant) profiel wordt nog niet ondersteund. We verwachten

---

[21] Zie voor meer details NL GOV Assurance profile for OAuth 2.0 v1.0 (centrumvoorstandaarden.nl)
[22] Zie voor meer details https://openid.net/specs/openid-igov-oauth2-1_0.html
[23] Verplichte standaarden | Forum Standaardisatie

wel dat een conceptversie met ondersteuning van een client credentials grant profiel voor het eind van 2022 beschikbaar komt.

5.3.1. Client typen/profiles

Het NL GOV OAuth Code Grant profiel[24] onderkent iets andere client profiles dan de OAuth-specificatie. Het gaat hier om een Full Client with User Delegation en een Native Client with User Delegation.

- Full Client with User Delegation:
  "*This client type applies to clients that act on behalf of a particular resource owner and require delegation of that user's authority to access the protected resource. Furthermore, these clients are capable of interacting with a separate web browser application to facilitate the resource owner's interaction with the authentication endpoint of the authorization server.*"

- Native Client with User Delegation:
  "*This client type applies to clients that act on behalf of a particular resource owner, such as an app on a mobile platform, and require delegation of that user's authority to access the protected resource. Furthermore, these clients are capable of interacting with a separate web browser application to facilitate the resource owner's interaction with the authentication endpoint of the authorization server. In particular, this client type runs natively on the resource owner's device, often leading to many identical instances of a piece of software operating in different environments and running simultaneously for different end users.*"

[24] Direct Access Clients worden (nu nog) uitgesloten