edustandaard

Edukoppeling

Identificatie en authenticatie

(ter besluitvorming)

Edustandaard

Status: ter besluitvorming

Datum: 12 maart 2018

Inhoudsopgave

1. Inleiding

Edukoppeling is door de Edustandaard gemeenschap geaccepteerd als het communicatieprotocol voor organisatie die werkzaam zijn in het onderwijs. De Edukoppeling standaard is gebaseerd op het nationale protocol Digikoppeling. Dit omvat de identificatie van de betrokken partijen met het zogenaamde Organisatie Identificerend Nummer (OIN).

In het onderwijs is het normaal geworden dat onderwijsinstellingen in de cloud werken met één of meerdere administraties. In dit verband hebben we het met name over SAAS-leveranciers (software-as-a-service) voor administratiesystemen . Deze administraties in de cloud wisselen vaak namens de onderwijsinstelling uit met andere instellingen, overheidsorganisaties of bedrijven.

Met de betrokkenen rond de werkgroep Edukoppeling is uitgebreid nagedacht over de soms best wel ingewikkelde situaties die daardoor ontstaan en hoe die in goede banen kunnen worden geleid. Deze best-practice is daarvan de weerslag.

1.1. Doel en doelgroep van dit document

Dit document heeft als doel ondersteuning te bieden bij Edukoppeling implementaties en is bedoeld voor medewerkers die bij de (technische) implementatie van Edukoppeling betrokken zijn. Het gaat hierom werknemers (ontwikkelaars, architecten, projectmanagers, informatiemanagers etc.) werkzaam bij onderwijsgerelateerde organisaties.

De lezer van dit document willen wij vragen om zaken die ontbreken of onduidelijk zijn te melden bij de beheerder van Edukoppeling (https://www.edustandaard.nl/standaarden/afspraken/afspraak/edukoppeling/).

1.2. Kernbegrippen

-identificatie

Identificatie is het kenbaar maken van de identiteit van een subject (een persoon/gebruiker of een proces/systeem). De identiteit op Edukoppeling is uniek en valideerbaar. De identiteit wordt gebruikt om de autorisatie (zie verder) - de toegang tot een service - te beheersen.

-authenticatie

Authenticatie is het proces waarbij nagegaan wordt of een subject daadwerkelijk is wie hij beweert te zijn, dat wil zeggen: daadwerkelijk de identiteit bezit die hij opgeeft. Bij de authenticatie wordt bijv. gecontroleerd of een opgegeven bewijs van identiteit overeenkomt met echtheidskenmerken. Het proces van authenticatie is dus onlosmakelijk verbonden met identiteit. Authenticatie levert als het ware de kwaliteit van de identificatie. Tevens speelt hier een 'chain of trust'. Als het 'root' certificaat van een PKI-certificaat te vertrouwen is (en het certificaat is niet ingetrokken of verlopen) dan mag men op de inhoud vertrouwen.

-autorisatie

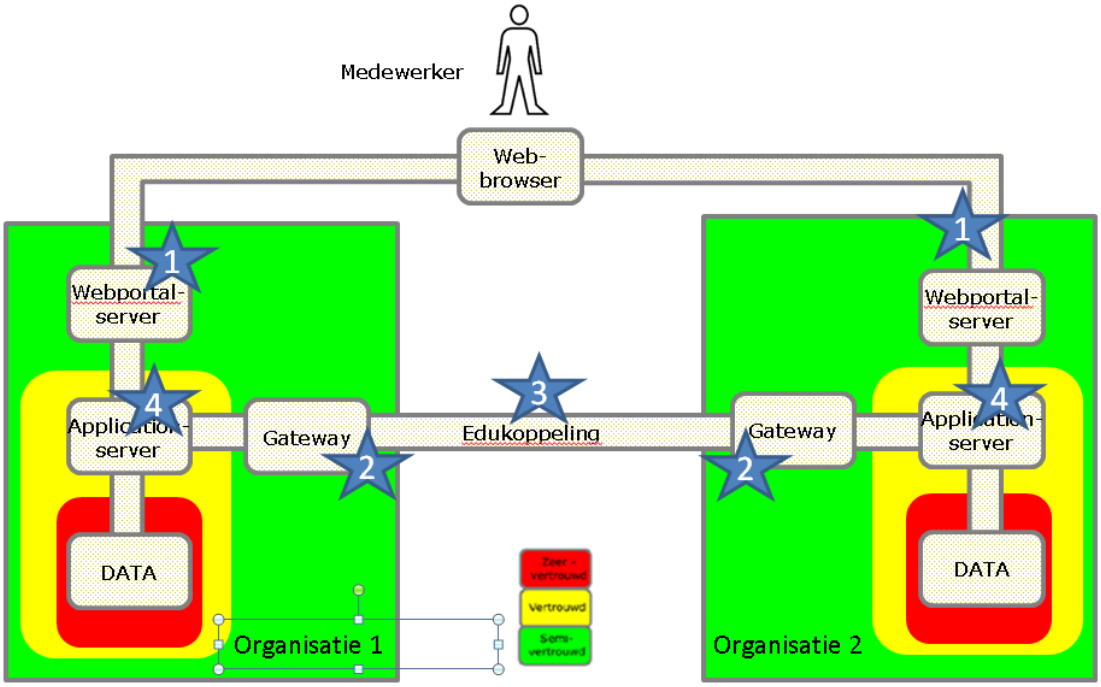
Autorisatie is het proces waarin een subject rechten krijgt op het benaderen van een service. De autorisatie wordt toegekend door de service-eigenaar. Het leidende principe (met name bij persoonsgegevens) is doelbinding: je mag alleen zien wat je voor je taak nodig hebt. Bij een collectieve informatievoorziening als deze geldt bovendien: je mag alleen je eigen dingen zien en niet de dingen van je collega-organisatie. De primaire reden voor het vaststellen van de identiteit van een subject is om op basis daarvan vervolgens vast te stellen of dat subject ook gerechtigd is om de gewenste service af te nemen. Die autorisatie (al of niet mede op basis van rollen, machtigingen, vertegenwoordigingen enzovoort) is nadrukkelijk een op de authenticatie volgende, aparte stap. De geauthenticeerde identiteit is dus nodig om autorisatie te kunnen doen. Autorisatie stelt eisen aan authenticatie.

-routering

Routering is kunnen bepalen van het (internet)adres waar een service aangeroepen kan worden. De inrichting van zo'n internetservice wordt in eerste instantie bepaald door de service-eigenaar, maar die dit in de regel uitbesteed aan ander, die in dit geval ook het inrichten van de applicatie in de cloud voor zijn rekening neemt. Dit komt precies, want ook hierbij geldt, het is niet de bedoeling dat privacygevoelige data op een verkeerde locatie wordt bezorgd. Vandaar dat de verantwoordelijke én de bewerker allebei een aandeel hebben in de goede werking van de routering. Als de relatie tussen die twee wordt verbroken, heeft dat per direct gevolgen voor het routeren van het berichtenverkeer.

2. Overzicht SAAS-model

In Figuur 1 is schematisch een beeld geschetst van ketensamenwerking. De school[1] is vertegenwoordigd in deze figuur als de organisatie die mensen in dienst heeft (de medewerker). Deze medewerker heeft bijvoorbeeld toegang tot een administratiesysteem in de cloud en tot bekostigingsgerelateerde informatie van DUO.



Figuur 1 - Schematische weergave ketensamenwerking

In de Edukoppeling architectuur zijn de elementen beschreven waaruit deze samenwerking bestaat. Een korte samenvatting:

1. In de front-office logt de medewerker van de school bij voorkeur in met een federatieve sleutel met een substantieel beveiligingsniveau (zoals een two-factor middel). De authenticatiefederatie is een vertrouwde derde partij die de *relatie* tussen medewerker en school kan valideren.
2. In de backoffice worden gegevens uitgewisseld conform de Edukoppeling standaard. De SaaS-leverancier is de partij die de uitwisseling feitelijk uitvoert in opdracht van de eindorganisatie (bijv. een school). De SaaS-leverancier beveiligt het verkeer (tweezijdig TLS) met een PKI-certificaat met eigen identificatie.

[1] Het begrip school wordt in dit gedeelte 'slordig' gebruikt. Het omvat termen als onderwijsinstelling en onderwijsaanbieder.

3. In een collectief serviceregister wordt bijgehouden (dat doet een medewerker van de school) of een organisatie is *gemandateerd* als bewerker van de uitgewisselde gegevens. Deze regelt het bijbehorende serviceverkeer namens de school.
4. Voor de beoordeling van de correcte werking van (cloud)systemen zijn normen beschikbaar. Dit is toegesneden op het uitwisselen met Edukoppeling.

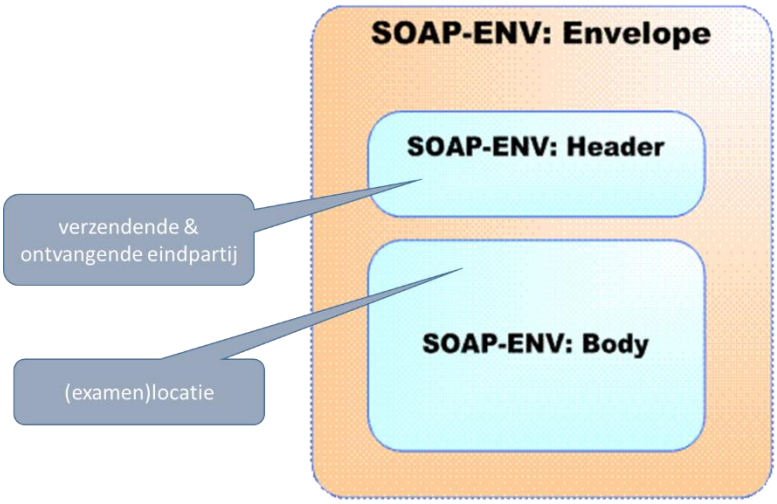
In de volgende paragraaf wordt ingegaan op de identificatie van de eindorganisatie (de functionele verzender/ontvanger).

3 Logistieke identiteit

In dit hoofdstuk wordt behandeld met identiteiten binnen Edukoppeling wordt omgegaan:

3.1 Header vs body

Edukoppeling is gebaseerd op SOAP. Een bericht bestaat daarin uit 2 onderdelen, een header en een body.



Figuur 2 - SOAP -onderdelen

Principe 1. Functie en logistiek zijn gescheiden in respectievelijk body en header. (of anders gezegd: Edukoppeling heeft geen boodschap aan de boodschap)

Een SAAS-leverancier kan diensten leveren aan meerdere scholen tegelijkertijd. Om die reden is in de Edukoppeling standaard afgesproken dat het zogenaamde Organisatie Identificerende Nummer (OIN) van de verzender en ontvanger van de school is opgenomen. Op basis hiervan kan de SAAS-leverancier achter de voordeur routeren.

Functionele aspecten waar de verwerkende applicatie iets mee moet, zitten per definitie in de body van het bericht. Bijvoorbeeld: als je leerlingen wilt kunnen tellen per school (zie verderop), dan wordt daarover in de body gecommuniceerd

Door deze strikte scheiding kan een ketenpartner “gelaagd” werken: een applicatie werkt met body (payload) en een gateway werkt met de header (adressering). Dat is relevant als een organisatie een complex applicatielandschap heeft. De scheiding in lagen is in het geval van DUO bijvoorbeeld oo scheiding in beveiligingszones.

3.2 School of rechtspersoon

Het OIN is volgens de definities van Digikoppeling een identiteit van 20 karakters. In deze systematiek is ruimte voor BRIN. Het volgende schema is ontleend aan Digikoppeling.

Prefix	Nummer	Suffix
00000001	RSIN uit het Handelsregister (9 posities)	"000"
00000002	RSIN of FI-nummer (9 posities)	Volgnummer (3 posities)
00000003	KvK nummer (8 posities)	Volgnummer "0000" (4 posities)
00000004	Nummer van Logius-beheerder (9 posities)	Volgnummer of "000" (3 posities)
00000005	Niet toegewezen	
00000006	Niet toegewezen	
00000007	Gereserveerd voor BRIN	
00000008 t/m 00000098 en vanaf 00000100	Nog niet toegewezen	
00000099	Reservering (9 posities)	Volgnummer (3 posities)

Het Register Instellingen en Opleidingen (RIO) is de boogde opvolger van het register BRIN.

Principe 2. Het OIN kan worden gevalideerd bij een nationaal of sectoraal register

(met als consequentie: het OIN biedt rechtszekerheid in het economisch verkeer)

Bedrijven, overheidsorganisaties en bevoegd gezagen kunnen op Edukoppeling opereren met een OIN dat is ontleend aan het handelsregister. In de onderwijspraktijk en -wetgeving is het gebruikelijk dat “kleinere eenheden” zelfstandig opereren. Daarvoor kennen we nu het register BRIN dat is gekoppeld aan het NHR. Volgens bovenstaand schema mag daar ook een OIN op worden gebaseerd.

Voor OIN's wordt centrale toegang geregeld door Logius. Dit heet de Centrale OIN Registratie (COR). Ook OIN's uit het onderwijsdomein worden op die manier toegankelijk.

In Doorontwikkelen BRON wordt gewerkt aan een opvolger van BRIN: het Register Instellingen en Opleidingen (RIO). In RIO gaan "scholen" over hun eigen identiteit en indeling. Aangenomen wordt dat de school die worden geregistreerd op eigen gezag uitwisselen met ketenpartners en dat het OIN daarvan wordt afgeleid. Vooralsnog zitten we in overgangsperiode en maken gebruik van de formele BRIN-structuur.

Ook de SAAS-leveranciers hebben in het SAAS-model een OIN gebaseerd op he handelsregister. Dit komt niet terug in de soap-header van het bericht, maar wel in het PKI-certificaat voor het beveiligen van het verkeer én in het serviceregister voor het valideren van de bewerkersrelatie met de school.

3.3 Administraties[2]

Zoals in de inleiding gezegd, veel scholen hebben een administratie in de cloud. In het verleden is wel gewerkt met de aanname dat scholen administraties bij houden per vestiging, maar dat wringt. Scholen hebben hun eigen afwegingen waarom ze één of meer contracten met SAAS-leverancier afsluiten of zelf met verschillende SAAS-leveranciers. Ook samenwerking van scholen kan invloed hebben op de administratieve indeling.

Principe 3. Een school bepaalt zonder restricties welke administratieve hij hanteert. (ergo: dit kan niet worden gebaseerd op criteria als geografie, onderwijsniveau of leerjaar, wet)

Omdat scholen ook samen een administratie kunnen voeren, wordt krijgt dit een eigen identiteit dat onafhankelijk is van de identiteit van deze samenwerkende scholen. Volgens dit principe registreren scholen welke administraties ze voeren. Deze registratie wordt gebruikt om een OIN op te baseren dat wordt gebruikt in de SOAP-header van Edukoppeling.

Dit heeft de volgende praktische consequenties:

1) Bij een uitwisseling waarbij het eerste contact uitgaat van de school, BRON is daarvan een voorbeeld, wordt door de ketenpartner(s) per keten per leerling/student de identiteit van de administratie onthouden. Dat is nodig om in latere instantie een bericht de andere kant op te kunnen sturen over die leerling/student.

2) Als het eerste contact uitgaat van een andere partij dan de school, bijvoorbeeld een nieuwe school wil een dossier opvragen bij de oude school, dan heeft de nieuwe school een lijst nodig met de door de oude school gevoerde administraties. Dit zal een openbare lijst worden. Aanbevolen wordt om bij een administratie een vrije omschrijving te geven van de populatie.

[2] In de praktijk wordt ook de term aanleverpunt gebruikt. Die wordt hier niet overgenomen omdat dit éénrichtingsverkeer suggereert.

3.4 Opbouw van het OIN

Partijen worden uniek geïdentificeerd aan de hand van een OIN (Overheids identificatie nummer). Het OIN bestaat altijd uit 20 posities en bestaat uit een aantal vaste onderdelen: “de prefix”, “hoofdnummer” en “suffix”.

Bijvoorbeeld ‘00000007’(prefix) + de BRIN (3 voorloopnullen, BRIN = 4 posities + 00, hoofdnummer) + het administratienummer (3 posities, suffix). Het OIN van voor het afgeleide administratiepunt komt er als volgt uit te zien: “0000000700025MB00**003**”. Het administratienummer mag in principe door de instelling/SAAS-leverancier zelf worden bepaald.

Principe 4. Dit administratienummer is uniek per BRIN binnen de keten. (ergo: het kan worden hergebruikt voor verschillende processen die een beroep doen op dezelfde administratie)

Elk administratiepunt binnen dezelfde instelling zal dan in gezamenlijk overleg een andere suffix gebruiken in het OIN om de uitwisseling met DUO en eventuele andere ketenpartners mogelijk te maken. Het OIN identificeert zowel de organisatie (het hoofdnummer) als de administratie (de suffix). Dit is terug te vinden in de technisch/logistieke laag van de berichtuitwisseling, de zogenaamde wsa:to en wsa:from headers.

In principe is het mogelijk dat deze werkwijze op termijn migreert van de uit vier karakters bestaande brincode (erkende onderwijsinstelling) naar de uit 7 karakters bestaande omschrijving van een onderwijsorganisatie (onderwijsaanbieder). Hiervoor zullen de ontwikkeling en vulling van het project RIO nauwgezet worden gevolgd.

Bovenstaande opbouw beschrijft een OIN op basis van een BRIN nummer. OIN’s kunnen op meerdere manieren worden opgebouwd. De prefix zal dan verschillen. Een OIN op basis van het KvK nummer zal de volgende prefix bevatten: “00000003”. Een softwareleverancier zal dit nummer bijvoorbeeld kunnen gebruiken voor de uitwisseling. Zij beschikken immers niet over een BRIN. Voor DUO geldt het volgende OIN 00000001800866472000.

4 Afronding

De Edukoppeling standaard heeft expliciete voorschriften over hoe partijen elkaar kunnen herkennen in het machine-machine berichtenverkeer. Deze afspraken zijn tot stand gekomen onder paraplu van de nationale standaard Digikoppeling. Edukoppeling is verder uitgewerkt vanuit het aspect cloud-computing.

Het verwachte resultaat is een openbare en enkelvoudige ‘adressenlijst’ die iedereen kan gebruiken die digitaal wil communiceren met een organisatie in het onderwijsveld. Initieel kan deze lijst worden gebaseerd op specifieke lijstjes van BRON, OSO en anderen. Nadat deze bijeen zijn gevoegd, ligt het onderhoud van een belangrijk deel bij de scholen.