edustandaard

Memo

Voor:	Werkgroep Edukoppeling
Van:	Bureau Edustandaard
Datum	25 september 2015
Betreft	Eerste analyse van oplossingsrichtingen voor IDM medewerker onderwijsinstelling

1. Inleiding

SaaS leveranciers geven aan dat de IDM voor medewerkers van onderwijsinstellingen die gebruik maken van hun diensten goed geregeld moet zijn, willen zij de verantwoordelijkheid kunnen nemen voor de e2e beveiliging die bovenop de toepassing van Edukoppeling gewenst is. Meer specifiek heeft dit betrekking op het kunnen gebruiken van een betrouwbare identiteit van de medewerker, de relatie van deze medewerker met een bepaalde onderwijsinstelling en de bevoegdheid om namens deze instelling een bepaalde dienst te mogen afnemen.

Er is aan de SION IAA werkgroep gevraagd te onderzoeken wat de mogelijkheden voor de inrichting hiervan zijn en met een voorstel te komen. We willen betrokken partijen zoveel mogelijk ontlasten en een generieke voorziening/oplossing heeft dus de voorkeur. Een aantal SION IAA werkgroepleden hebben een eerste inventarisatie gedaan die in de werkgroep van 9 september 2015 aan de orde is gekomen zowel in een aparte presentatie als in de discussie rond de rol van PKI-certificaten. In deze memo is de genoemde presentatie iets verder uitgewerkt. De inventarisatie heeft de volgende inzichten en vragen opgeleverd.

2. Mogelijke oplossingsrichtingen

Er zijn verschillende generieke voorzieningen waarmee het IDM & het bevoegdheid vraagstuk ingevuld zou kunnen worden, dit zijn bijvoorbeeld:

1. eHerkenning, eID/Idensys
2. Federatie en IdP onderwijsinstelling (Kennisnetfederatie, SURFConext)

Ook kunnen beschikbare voorzieningen meer generiek toegepast gaan worden, zoals:

3. DUO zakelijk portaal
4. Commercieel product

Daarnaast kan er ook gekeken worden hoe IDM momenteel bij SaaS leveranciers is ingericht en of dit ook bij toepassing van Edukoppeling gehandhaafd kan blijven.

5. Huidige werkwijze voortzetten

2.1. eHerkenning / eID/Idensys

Omdat er nog onduidelijk is hoe het huidige eHerkenning zich tot eID/Idensys gaat verhouden worden deze hier apart toegelicht. Daarnaast biedt eHerkenning nu al diensten en is eID/Idensys nog theory

2.1.1. eHerkenning

Er zijn al eHerkenning diensten beschikbaar die de benodigde functies bieden, er kan betrouwbaar een identiteit door het stelsel geleverd worden waarbij ook de bevoegdheid om namens de dienstafnemer (school) deze dienst bij de dienstverlener af te nemen. De SaaS leverancier zich

edustandaard

moeten registreren als dienstaanbieder van bepaalde diensten in de dienstencatalogus en de school zal de machtigingen moeten registreren in het machtigingenregister. Voor authencitatiemiddelen van de gebruiker worden kosten in rekening gebracht. eHerkenning is een stelsel voor het organisatiedomein en staat eigenlijk los van het burgerdomein. Hiermee zijn de middelen niet noodzakelijk aan een persoon binnen organisatie gekoppeld maar meer waarschijnlijk een rol die door meerdere mensen ingevuld kan worden. Hiermee ontstaat de kans dat er minder zorgvuldig met dit middel omgegaan wordt.

eHerkenning onderkent momenteel niet het gewenste identificatieniveau (onderwijsinstelling/afleverpunt), maar enkel bevoegd gezag/rechtspersoon (RSIN/KvK/OIN). Wanneer deze optie toegepast kan worden is dus afhankelijk hoe snel er binnen het afsprakenstel wijzigingen doorgevoerd kunnen worden om scholen goed te kunnen identificeren.

Er zou nu onderzocht kunnen worden of eHerkenning op termijn aan een aantal wensen vanuit het onderwijs tegemoet wil komen en wat hier de verwachtte doorlooptijd is.

2.1.2. eID / Idensys

eID is nog theorie, de werking zoals in afsprakenstelsel 2.0 beschreven is voorlopig nog niet beschikbaar. Verder biedt men ook geen zekerheid in hoeverre de realisatie van eID hierop gebaseerd wordt.

De theorie belooft wel oplossing voor processen waar hogere betrouwbaarheid vereist wordt. In de toekomst kan dan ook waarschijnlijk binnen het onderwijs gebruik worden gemaakt van het eID stelsel. Doordat men nu voor ogen heeft eHerkenning door te ontwikkelen naar het eID stelsel, zou het nu gebruiken van eHerkenning middelen de integratie met eID al een stap dichterbij brengen. Er zijn momenteel geen andere concrete eID oplossingen.

2.2. Koppeling met Federatie en IdP onderwijsinstelling

Binnen het onderwijs zijn er al generieke voorzieningen, zoals Kennisnet Federatie en SURFConext. Deze maken gebruik van de IdP van een onderwijsinstelling. Deze IdP kan een eigen voorziening betreffen (bijvoorbeeld ADFS), maar kan ook bij een leverancier belegd zijn. De school is wel verantwoordelijk voor de registratie van gebruikers. Binnen het PO, VO en MBO wordt de Kennisnet Federatie gebruikt en bij MBO en hoger de SURFconext federatie.

Er zou onderzocht kunnen worden hoe onderwijsinstellingen in alle sectoren een betrouwbare identiteit aan een federatie kunnen leveren met hieraan gekoppeld een aantal betrouwbare attributen zoals ‘Rol’ en ‘Onderwijsinstelling’. Door de Rol te formaliseren kan dit samen met het attribuut Onderwijsinstelling gezien worden als een machtiging namens de betreffende school.

Het is nu onduidelijk wat er bij een onderwijsinstelling geregeld moet worden om dergelijke identiteiten en attributen betrouwbaar te kunnen leveren. Dit zal ook sterk per sector verschillen (PO/MBO). Een alternatief om eea meer centraal te regelen zou het gebruik van Kennisnet Entree IdP kunnen zijn indien deze aan een hoger betrouwbaarheid gaat voldoen. Deze en andere varianten zouden samen met Kennisnet / LAS leverancier en een aantal onderwijsinstellingen onderzocht kunnen worden.

2.3. DUO Zakelijk portaal

DUO heeft voor haar eigen dienstenplatform al een IdP ingericht. De gebruikers van deze diensten komen voor een groot deel overeen met de gebruikers die namens onderwijsinstellingen via een SaaS dienst gegevens verwerken en verstrekken. Van deze gebruikersgroep is de identiteit en de relatie van gebruiker met de onderwijsinstelling betrouwbaar vastgesteld. Hiermee beschikken zij dus al over een

middel waaraan een pseudoniem voor de LAS leverancier gekoppeld kan worden, eventueel middels een federatieve koppeling.

Het probleem bij deze variant is echter dat de IdP nu integraal onderdeel uitmaakt van het dienstenplatform. Er zou dus een project gestart moeten worden om externe diensten aan te kunnen sluiten (eventueel via federatieve koppeling).

2.4. Commercieel product

Er zijn vele ontwikkelingen in de markt rond identiteiten- en attributenleveranciers. Vanuit het onderwijs wordt een commercieel product niet uitgesloten, tenslotte bestaan stelsels zoals eHerkenning ook uit een publieke/private samenwerking.

Binnen het onderwijs ontbreekt het echter momenteel nog aan een afsprakenstelsel waar deze partijen zich aan zouden moeten houden zodat er garanties zijn rond de eisen die vanuit het onderwijs gesteld worden. De stelselgedachte is ook binnen het onderwijs wel in ontwikkeling en vanuit het SION IAA persoonsidentiteiten project zijn al uitgangspunten hiervoor geformuleerd.

Er wordt verwacht dat de gebruikers nog niet een middel/identiteit hebben bij een mogelijke marktpartij en het is nog minder waarschijnlijk dat er een mandaat relatie met de onderwijsinstelling beschikbaar is.

Er zou onderzocht moeten worden welke marktpartijen passende diensten leveren en in hoeverre deze binnen een in ontwikkeling zijnde IAA stelsel onderwijs passen.

2.5. Huidige werking IDM bij leveranciers

Het is nu niet duidelijk wat de huidige werkwijze van SaaS leveranciers rond IDM van medewerkers van onderwijsinstellingen is. Er worden nu certificaten gebruikt, maar hoe deze informatie aan de ingelogde gebruiker wordt gekoppeld is nog niet bekend. Wel is bij overleg van Edukoppeling WG van september duidelijk geworden dat indien er geen goed passend alternatief geboden wordt er nog steeds schoolcertificaten nodig zijn ook al worden deze niet meer gebruikt voor versleuteling van de m2m koppeling.

3. Conclusie

Het is duidelijk dat er nog geen perfecte oplossing naar voren gekomen is, alle besproken varianten vragen een zeker termijn voordat deze toegepast kunnen worden, waarbij de mate van zekerheid rond dit termijn sterk varieert.

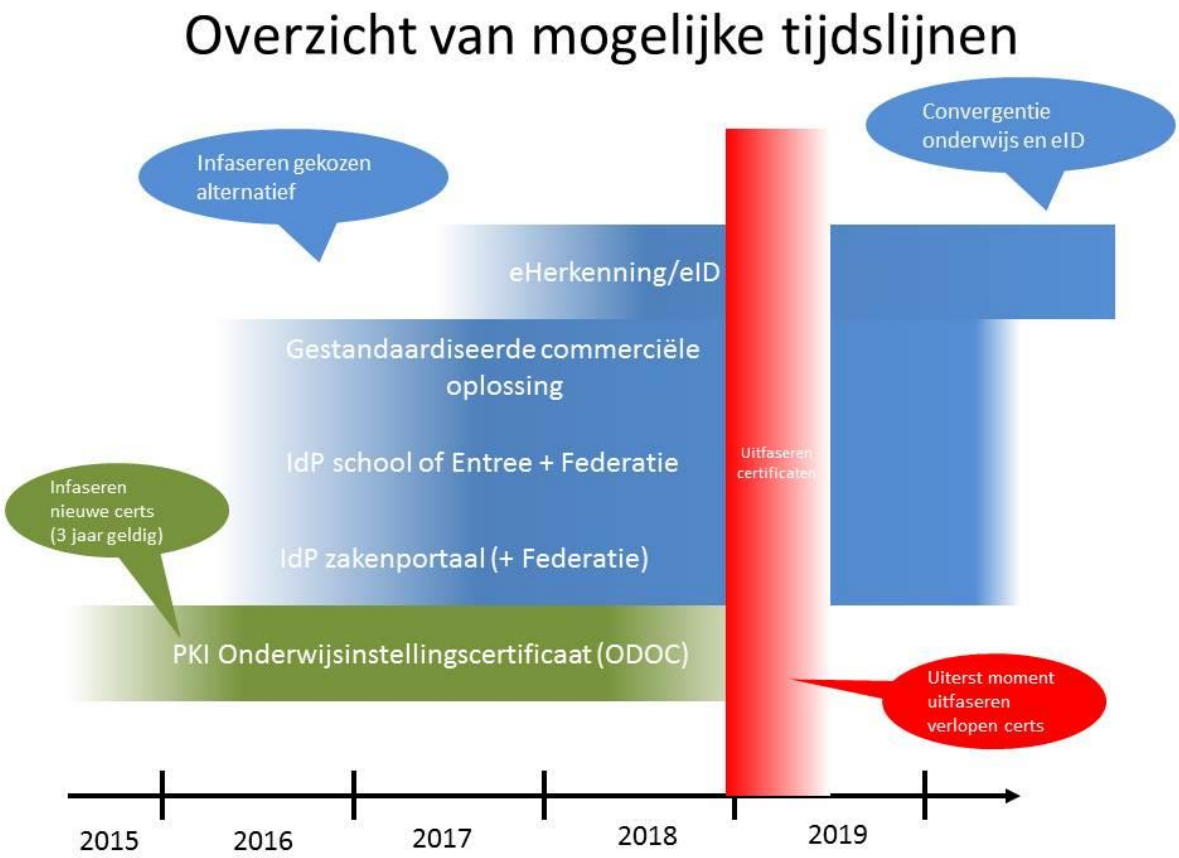
Op basis hiervan en de Edukoppeling WG bijeenkomst van september kan wel gesteld worden dat er nog steeds met onderwijsinstellingscertificaten gewerkt moet worden. Deze kunnen in meerdere toepassingsgebieden gebruikt worden waar een handelende partij bij het gebruik van een SaaS dienst aan een onderwijsinstelling gekoppeld moet kunnen worden. Dit certificaat wordt door de SaaS leverancier conform Edukoppeling 1.2 dan niet gebruikt voor de m2m koppeling met externe partijen, hiervoor wordt het eigen SaaS certificaat gebruikt.

Handhaving van het gebruik van onderwijsinstellingscertificaten lijkt mogelijk gezien er plannen zijn om deze tijdig in de verschillende sectoren beschikbaar te stellen. Dit zou dan een oplossing kunnen zijn voor de periode dat deze nieuwe certificaten geldig zijn (3 jaar). Er zou samen met LAS leverancier onderzocht kunnen worden op welke vlakken er wel gestandaardiseerd kan worden. Hoe

edustandaard

is het proces rond registratie van dat certificaat bij SaaS leverancier en hoe wordt de identiteit van de handelende partij hieraan gekoppeld?

4. Overzicht alternatieven



Figuur 1- Overzicht alternatieven (er ge