saMBO-ICT

Implementatie ECK-ID in het mbo

Onderzoek naar de belemmeringen bij de implementatie van het ECK-ID in het mbo

Bas Kruiswijk
Versie 0.3, 23 maart 2021

Versiebeheer

Versie	Datum	Opmerkingen
0.1	22-02-2021	Eerste versie na interviews
0.2	11-03-2021	Aanpassingen n.a.v. bespreking met Maaike Stam, Marc Dietzenbacher, Merijn van der Schoot en Erwin Pelt.
0.3	23-03-2021	Aanpassingen n.a.v. bespreking met Martijn Timmer

Inhoudsopgave

1. Inleiding

1.1 Inleiding

De afgelopen jaren is gewerkt aan de invoering van het ECK-ID in het po, vo en mbo om een betere privacybescherming in de leermiddelenketen te realiseren. In het po en vo maakt inmiddels een groot deel van de instellingen gebruik van het ECK-ID, terwijl de implementatie in het mbo fors achterblijft.

Dit rapport is het resultaat van een kort onderzoek naar de oorzaak van die vertraging. Op basis daarvan wordt ook een aantal aanbevelingen gedaan om de implementatie weer vlot te trekken.

1.2 Achtergrond

De invoering van het ECK-ID heeft tot doel om een betere privacybescherming en dataminimalisatie in de leermiddelenketen te realiseren. Dit wordt gedaan door een ketenpseudoniem, het ECK-ID in te voeren. Dit ECK-ID is voor partijen in de leermiddelenketen niet herleidbaar tot de persoonsgegevens van een student.

Het ECK-ID wordt via de zogenaamde Nummervoorziening centraal uitgegeven. De instelling kan dit ECK-ID opvragen en versleuteld opslaan in het Student Informatie Systeem (SIS). Vervolgens moet de instelling het ECK-ID verstrekken in de keten. Voor toegang tot de leermiddelenketen wordt in het mbo voornamelijk gebruik gemaakt van de Entree federatie. Studenten krijgen na authenticatie met hun schoolidentiteit toegang de leermiddelen. De instelling moet ervoor zorgen dat bij deze authenticatie uitsluitend het ECK-ID wordt verstrekt, en geen andere persoonsgegevens.

We gaan in dit rapport niet uitvoerig in op de werking van de Nummervoorziening en de Entree federatie. Daar is andere documentatie voor beschikbaar.

Evenmin wordt ingegaan op nut en noodzaak van het ECK-ID als zodanig.Het uitgangspunt is dat met de introductie van het ECK-ID scholen kunnen voldoen aan het Privacy Convenant. De technische voorschriften voor de Nummervoorzieningen het ECK-ID zijn kaderstellend voor de afspraken die in Edu-K verband zijn gemaakt.

1.3 Dit onderzoek

Het doel van dit onderzoek is om compact in kaart te brengen wat de impact van de implementatie van ECK-ID in het mbo is, waarom de implementatie in het mbo relatief moeizaam verloopt en wat gedaan kan worden om de implementatie in het mbo succesvoller te laten zijn.

1.3.1 Vraag

De vraag valt uiteen in een aantal deelvragen, die in deze notitie achtereenvolgens behandeld zullen worden.

- Wat houdt de implementatie van het ECK-ID in het mbo concreet in? Hoe lopen de gegevensstromen en bij welke partijen en in welke systemen moet er wat gebeuren?

- Wat zijn de blokkades voor een soepele implementatie vanuit het perspectief van de verschillende betrokken partijen, met name: de instellingen, de leveranciers (zowel van SIS- als IAM-toepassingen) en de betrokken ketenpartijen Edu-K, SEM, Kennisnet, MBO Raad en saMBO-ICT.
- Wat zijn concrete aanbevelingen om de implementatie in het mbo vlot te trekken?

1.3.2 Documentatie en interviews

Dit onderzoek vindt hoofdzakelijk plaats op basis van interviews. Er is uiteraard de nodige documentatie beschikbaar, maar het is vooral de vraag welke problemen in de praktijk worden ondervonden en wat de analyse van die problemen vanuit de verschillende invalshoeken is.

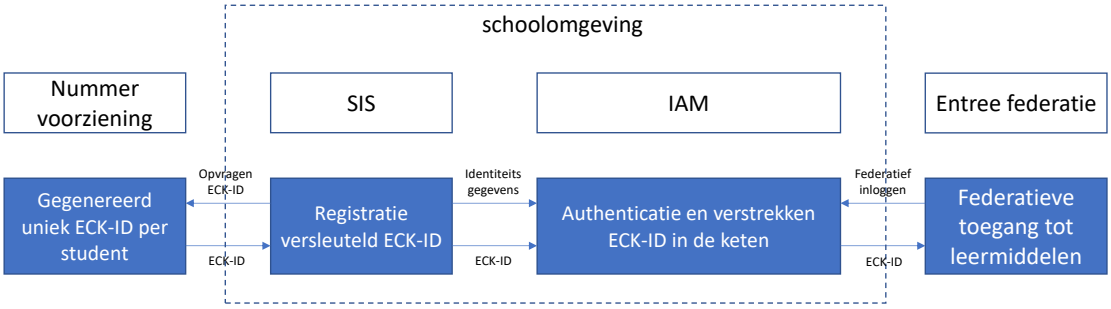
In de bijlage is een lijst opgenomen met de documentatie waarnaar in dit rapport wordt verwezen en een lijst met geïnterviewde betrokkenen.

2. Overzicht

In dit hoofdstuk wordt in het kort een overzicht gegeven van wat de implementatie van het ECK-ID in het mbo inhoudelijk is. We starten met een inhoudelijk afbakening, waarna wordt ingezoomd op de verschillende stappen. Ook wordt de tijdlijn van de invoering tot nu toe globaal geschetst.

2.1 Afbakening

Onder de invoering van het ECK-ID in het mbo wordt het proces verstaan dat start met het opvragen van het ECK-ID bij de nummervoorziening tot het verstrekken van het ECK-ID in de keten door middelen van federatieve authenticatie.



In het mbo hebben nagenoeg alle instellingen een aparte omgeving voor identiteits- en toegangscontrole (Identity and Access Management, IAM). Dat betekent dat het proces bestaat uit drie stappen.

1. Het SIS (Student Informatie Systeem) van de instelling vraag het ECK-ID van studenten en docenten op bij de Nummervoorziening en slaat het ECK-ID versleuteld op in het SIS
2. Het ECK-ID wordt uitgewisseld met de IAM-omgeving van de school en ook daar versleuteld opgeslagen zodat het beschikbaar kan worden gesteld bij authenticatie
3. Wanneer een student of docent toegang vraagt tot leermiddelen via de Entree federatie, dan wordt dat verzoek naar de IAM-omgeving van de instelling geleid. De instelling authentiseert de gebruiker en verstrekt het ECK-ID in de keten.

2.2 Inhoudelijk overzicht

We zoomen in op de drie hiervoor genoemde stappen.

2.2.1 Opvragen ECK-ID bij Nummervoorziening

De Nummervoorziening is een publieke dienst van Kennisnet. Met behulp van deze voorziening kan vanuit het SIS een ECK-ID worden aangevraagd voor een student of docent.

Om dit mogelijk te maken sluit de instelling een contract met Kennisnet voor het gebruik van deze dienst. De SIS-leverancier implementeert het koppelvlak op basis van de door Kennisnet gepubliceerde specificaties, die zijn gebaseerd op de EduKoppeling standaard.

Opvragen van het ECK-ID vindt kort samengevat in de volgende stappen plaats.

- In het bestaande proces voor aanmelding en inschrijving in het SIS wordt de identiteit van een student bij DUO gecontroleerd en een Persoonsgeboden Nummer (PGN) aangemaakt. In de meeste gevallen is dat gelijk aan het Burgerservicenummer (BSN), met uitzondering van bijvoorbeeld studenten die niet in Nederland wonen.
- Vanuit het SIS wordt een dienst van de Nummervoorziening aangeroepen om op basis van het PGN een stampseudoniem te creëren. Dit stampseudoniem wordt versleuteld in het SIS opgeslagen en niet uitgewisseld.
- Vanuit het SIS wordt vervolgens een dienst van de Nummervoorziening aangeroepen om op basis van het stampseudoniem een ketenpseudoniem, het ECK-ID te genereren. Er kunnen in principe meerdere ketenpseudoniemen worden gecreëerd voor hetzelfde stampseudoniem. Het ECK-ID wordt versleuteld in het SIS opgeslagen en kan in de keten worden uitgewisseld.

De SIS-leveranciers kunnen het opvragen van het ECK-ID op basis van de door Kennisnet gepubliceerde specificaties in het SIS implementeren.

2.2.2 Uitwisselen ECK-ID met IAM-omgeving

Nagenoeg alle mbo-instellingen hebben een aparte omgeving voor identiteits- en toegangscontrole (een Identity and Access Management (IAM) omgeving). In die omgeving vindt authenticatie van gebruikers plaats en worden identiteitsgegevens beschikbaar gesteld aan afnemende systemen waaronder de Entree federatie en de leermiddelenketen.

Dit betekent dat het ECK-ID moet worden uitgewisseld met de IAM-omgeving.

Als mbo-instellingen een aparte IAM-omgeving gebruiken, dan is er al een bestaand koppelvlak tussen het SIS en die IAM-omgeving. De manier waarop dat is geïmplementeerd verschilt per instelling. Meer dan de helft van de instellingen gebruikt Microsoft AD (Active Directory) en ADFS (Active Directory Federation Services). De wijze waarop de AD gevuld wordt vanuit het SIS verschilt ook nog sterk. Het kan rechtstreeks, maar vaak is er maatwerk gerealiseerd of wordt er een tussenproduct (vaak Microsoft MIM) gebruikt om identiteitsgegevens uit bronsystemen te verzamelen, autorisaties te beheren en vervolgens in de AD te plaatsen.

Er zijn ook instellingen die een ander product gebruiken, zoals Microfocus NetIQ. Dat geldt bijvoorbeeld voor een aantal scholen die het product Red Spider hebben laten ontwikkelen, dat nu bij KIEN-ICT in beheer is. Dit product voorziet in standaard koppelvlakken, onder andere met het SIS, om autorisaties te beheren en uit te wisselen. Authenticatie kan binnen NetIQ plaatsvinden, maar vaak wordt naast deze omgeving ook nog een AD met ADFS gebruikt waar de daadwerkelijke authenticatie plaatsvindt.

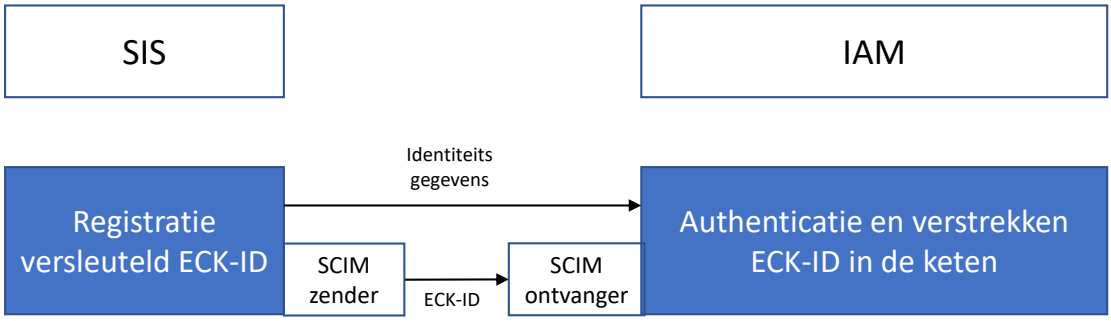
Tenslotte is er nog een beperkt aantal instellingen met andere oplossingen, zoals Tools4Ever, IDfocus of Brite. De inschatting is dat het gebruik van deze omgevingen minimaal is.

In principe zijn er drie mogelijkheden om het ECK-ID uit te wisselen tussen het SIS en de IAM-omgeving. Deze mogelijkheden zijn ook beschreven in een advies van het Ketenarchitectuurteam (KAT).

1) Realiseren van een nieuw koppelvlak op basis van de UWLR-L standaard
2) Realiseren van een apart koppelvlak voor het ECK-ID op basis van SCIM
3) Uitbreiden van het bestaande koppelvlak met het ECK-ID, en dit afdoende beveiligen op basis van TLS 1.2

Optie 1 (UWLR) is een onderwijs-specifiek protocol en daardoor lastig te implementeren in generiek IAM-omgevingen zoals ADFS. Optie 2 (SCIM, System for Cross-domain Identity Management) wordt geadviseerd omdat het een internationale standaard is. Maar dit betekent wel dat het ECK-ID apart, dus naast het bestaande koppelvlak wordt uitgewisseld. Optie 3 is wel toegestaan volgens de vereisten van de Nummervoorziening, maar wordt in het advies van het Ketenarchitectuurteam (KAT) afgeraden als "vanuit efficiëntie overwegingen en vanuit de AVG niet wenselijk (teveel verschillende maatwerkkoppelingen)"

Op basis hiervan is door Edu-K in alle communicatie naar scholen en leveranciers uitgegaan van het hieronder weergegeven koppelvlak op basis van SCIM.



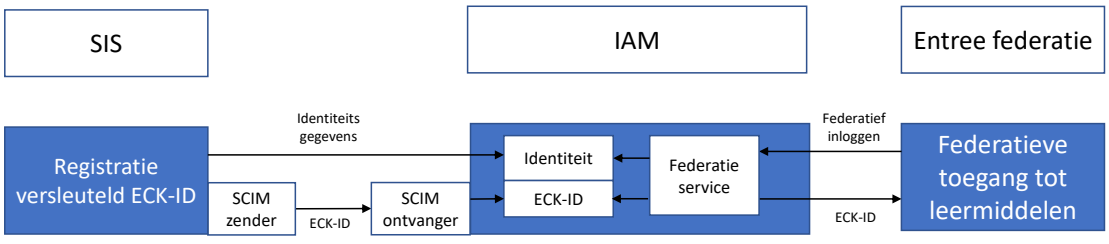
De voorgestelde oplossing is dus om de uitwisseling van identiteitsgegevens tussen SIS en IAM-omgeving te laten zoals die is, en daarnaast een koppelvlak voor het ECK-ID te introduceren op basis van het SCIM protocol.

Het SCIM-protocol is bijzonder in de zin dat het een push mechanisme is vanuit het SIS. In het SIS moet een SCIM-zender worden geïmplementeerd die een gecreëerd ECK-ID publiceert, wat aan de kant van het IAM door een SCIM-ontvanger kan worden ontvangen en verwerkt.

Het ECK-ID moet vervolgens versleuteld in de IAM-omgeving worden opgeslagen.

2.2.3 Authenticatie en verstrekken ECK-ID in de keten

In de IAM-omgeving vindt vervolgens de authenticatie plaats en wordt na authenticatie het ECK-ID verstrekt zonder andere persoonsgegevens. In de leermiddelenketen wordt op die manier de student en docent geïdentificeerd zonder dat er persoonsgebonden gegevens nodig zijn, met een ID dat ook niet tot die persoonsgegevens te herleiden is. Alleen de instelling kan op basis van de gegevens in het SIS het ECK-ID herleiden tot de bijbehorende persoonsgegevens.



Startend rechts op deze afbeelding is het proces als volgt.

- Wanneer een student of docent toegang wil tot een leermiddel, dan wordt dit via de Entree federatie teruggeleid naar de federatie service (bijvoorbeeld ADFS) van de betreffende instelling.

- Er vindt authenticatie plaats op basis van de geregistreerde identiteiten (bijvoorbeeld de AD)
- De eventueel benodigde attributen, waaronder het ECK-ID worden verzameld
- Het ECK-ID wordt terug geleverd aan de Entree federatie zodat het in de keten kan worden gebruikt

Een belangrijke eis hierbij is dat het ECK-ID in de IAM-omgeving versleuteld moet worden opgeslagen, zodanig dat het door de federatie service weer kan worden verstrekt.

Het IAM is bij instellingen in het mbo heel verschillend ingericht. In de meerderheid van de instellingen wordt gebruikgemaakt van ADFS en/of Azure AD als federatie-service. Het blijkt dat er in die omgeving geen eenvoudige oplossing is voor het versleutelen en weer verstrekken van het ECK-ID. Wanneer het ECK-ID versleuteld in de AD is opgeslagen, dan is het met ADFS en Azure AD niet mogelijk om dit attribuut bij authenticatie direct te ontsleutelen en in de keten te verstrekken.

Er zijn ook scholen die een ander product in hun IAM-omgeving gebruiken, zoals bijvoorbeeld Microfocus NetIQ (waarop ook het RedSpider-product is gebaseerd). Wanneer NetIQ ook als federatie service wordt gebruikt, dan doet dit probleem zich niet voor. Met NetIQ is het wel mogelijk om een versleuteld ECK-ID bij authenticatie direct te ontsleutelen en in de keten te verstrekken.

Kennisnet heeft een aanvullende handreiking opgesteld voor instellingen die van Microsoft AD, ADFS en/of Azure AD gebruik maken (Handreiking ECK-ID in Active Directory). Hierin worden drie scenario's beschreven.

1. Het ECK-iD wordt in een aparte en afdoende beveiligde database opgeslagen.

   In dit scenario wordt het ECK-ID niet in de AD, maar in een aparte beveiligde database opgeslagen. Ten behoeve van de authenticatie wordt ADFS zo ingericht dat het ECK-ID apart wordt opgevraagd (met een zgn. tweede claim rule), waarbij de ontsleuteling wel automatische kan plaatsvinden. In dit scenario kan gebruik worden gemaakt van de standaardfunctionaliteit van SQL-Server voor het versleutelen en ontsleutelen.

   Deze oplossing werkt alleen in combinatie met ADFS en niet met Azure AD.

2. Het ECK-iD wordt versleuteld opgeslagen in Active Directory.

   In dit scenario dient een aanvullende middleware-applicatie te worden geïmplementeerd om het ECK-ID bij het opslaan in de AD te versleutelen en bij het opvragen door ADFS bij authenticatie weer te ontsleutelen.

3. Het ECK-iD wordt versleuteld opgeslagen in een Azure Active Directory omgeving.

   In dit scenario wordt er net als in scenario 1 een aparte database voor het ECK-ID ingericht, maar dan in de Azure omgeving. Daarnaast is een aanvullende middleware-applicatie nodig om het ECK-ID bij het opslaan te versleutelen en bij het opvragen bij authenticatie weer te ontsleutelen.

Zowel scenario 2 als scenario 3 vereisen dat er aanvullende middleware wordt ingezet die het ECK-ID versleutelt voordat het wordt opgeslagen, en weer ontsleutelt wanneer het door ADFS of Azure AD wordt opgevraagd. Hiervoor zijn geen standaardoplossingen in de markt beschikbaar.

Scenario 1 blijkt voor de meeste instellingen het best praktisch te realiseren. Er is geen aanvullende middleware nodig om te versleutelen en ontsleutelen omdat dit ondersteund door standaard database technologie zoals SQL-Server. Een complexiteit van dit scenario is wel dat ADFS zodanig moet worden geconfigureerd dat naast de authenticatie op de AD een aparte actie (claim) moet worden uitgevoerd om het ECK-ID uit de aparte database op te vragen. Ook ditis standaard functionaliteit, die overigens niet formeel door Microsoft wordt ondersteund als de database in de (Azure) cloud staat.

2.3 Tijdlijn

Dit onderzoek is geen uitgebreide reconstructie van de tijdlijn en de stappen die gezet zijn. Voor de context wordt hier een kort overzicht gegeven.

- Eind 2018: Overeenstemming binnen Edu-K over de belangrijkste architectuurkeuzes, zodat marktpartijen en instellingen kunnen realiseren en implementeren
- Maart 2019: Iddink als eerste leverancier gereed met implementatie van het ECK-ID in EduArte
- Zomer 2019: Eerste mogelijkheid voor instellingen om te implementeren, maar dit bleek voor geen van de instellingen haalbaar
- Mei 2020: Oracle ook gereed met implementatie van het ECK-ID in Peoplesoft Campus Solutions
- Voorjaar 2020: Ketentest van Iddink met een aantal instellingen
- Zomer 2020: Laatste mogelijkheid voor instellingen om nog met ondersteuning vanuit Edu-K te implementeren. Zeer beperkt aantal instelling heeft geïmplementeerd

3. Analyse

Dit hoofdstuk is de analyse van de belangrijkste blokkades en knelpunten die een soepele implementatie van het ECK-ID in het mbo belemmeren. We maken hierbij onderscheid tussen inhoudelijk belemmeringen, belemmeringen in de organisatie en aansturing van het geheel, en belemmeringen ten aanzien van kosten.

3.1 Inhoudelijk

Inhoudelijk wordt de analyse gesplitst in drie deelgebieden.

3.1.1 SIS

De aanpassingen in het SIS betreffen het opvragen van het ECK-ID bij de nummervoorziening en het realiseren van een SCIM-zender voor het verstrekken van het ECK-ID aan de IAM-omgeving of het uitbreiden van de bestaande koppelvlak met de IAM-omgeving.

SIS leveranciers hebben aangegeven dat het op basis van de specificaties voor hen mogelijk is om de noodzakelijke aanpassingen in hun oplossing door te voeren.

Voor wat betreft het koppelvlak met de nummervoorziening geven de leveranciers aan dat dit op basis van de specificaties zonder problemen geïmplementeerd kan worden. In EduArte, Magister en Peoplesoft is de koppeling beschikbaar. De andere SIS-leveranciers (CACI en EducationOnline) geven aan dat het op hun roadmap staat en dat het afhankelijk van de vraag van instellingen kan worden geïmplementeerd.

Voor wat betreft de koppeling met de IAM-omgeving is de situatie complexer. Leveranciers zullen een SCIM-zender moeten implementeren, of het ECK-ID moeten toevoegen aan hun bestaande koppeling met een IAM-omgeving. Alleen Iddink heeft de SCIM-zender als additioneel koppelvlak beschikbaar, en voor Peoplesoft is door een van de instellingen (ROC van Twente) de complete SCIM-koppeling gerealiseerd, die ook aan andere instellingen beschikbaar kan worden gesteld. De andere SIS-leveranciers (CACI en EducationOnline) geven aan dat het op hun roadmap staat en dat het afhankelijk van de vraag van instellingen kan worden geïmplementeerd.

Inhoudelijk lijken er geen belemmeringen bij de SIS-leveranciers te zijn om zowel de koppeling met de nummervoorziening als met het IAM van de instellingen te realiseren. Er zijn wel twijfels over de wenselijkheid van het gebruik van de SCIM-standaard. Mogelijk dat leveranciers ervoor kiezen om de koppeling met het IAM van de instelling op een andere wijze te implementeren.

3.1.2 IAM

De aanpassingen in de IAM omgeving betreffen het ontvangen van het ECK-ID van het SIS door middel van een SCIM-ontvanger of via het bestaande koppelvlak met het SIS. Het ECK-ID moet versleuteld en de IAM-omgeving worden opgeslagen en van de federatie service van de instelling (meestal ADFS) en de Entree federatie in de keten beschikbaar worden gesteld.

De IAM-omgevingen zijn in het mbo heel divers en instellingen doen vaak veel zelf. Bovendien zijn er nauwelijks IAM-leveranciers die voor dit vraagstuk een pasklare oplossing beschikbaar hebben die instellingen zouden kunnen aanschaffen.

De instellingen moeten daarom zelf op zoek naar een passende oplossing.

Het grootste deel van de instellingen gebruikt een omgeving op basis van Microsoft AD en ADSF, soms in combinatie met Azure AD. Zowel ADFS als Azure AD bieden geen standaard oplossing voor het versleuteld opslaan en verstrekken van het ECK-ID. Er is complexe inrichting en/of maatwerk nodig om het geheel te laten werken.

Een beperkt aantal instellingen maakt gebruik van andere producten, zoals RedSpider (gebaseerd op NetIQ in plaats van Microsoft AD en ADFS). In die omgeving is de implementatie minder complex. Met name omdat NetIQ wel een standaard oplossing biedt voor het versleuteld opslaan en verstrekken van het ECK-ID.

Gaandeweg is meer duidelijkheid ontstaan over de manier waarop de IAM-omgeving moet worden ingericht. In een Microsoft omgeving lijkt daarbij die inrichting van een aparte database voor het ECK-ID de beste oplossing. Er zijn op dit moment een paar succesvolle implementaties bekend.

- Het ROC van Amsterdam gebruikt EduArte. Zij hebben door DWE-ICT een SCIM-ontvanger en de aparte database voor het ECK-ID laten realiseren. Op basis daarvan is nu ADFS ingericht zodat het ECK-ID aan de Entree federatie kan worden doorgegeven
- Het ROC van Twente gebruikt Peoplesoft. In het RedSpider product dat zij gebruiken, is zowel de SCIM-ontvanger als het versleuteld opslaan en verstrekken van het ECK-ID gerealiseerd.
- IT-Workz biedt een oplossing voor instellingen op basis van Microsoft AD en ADFS. IT-Workz heeft zowel de SCIM-ontvanger als de aparte database voor het ECK-ID gerealiseerd zodat deze versleuteld kan worden opgeslagen en in de keten kan worden verstrekt. Deze oplossing wordt vooralsnog alleen door het Nordwin college gebruikt.

3.1.3 Educatieve keten

In de Educatieve keten is het noodzakelijk dat de Entree federatie zodanig wordt aangepast dat bij authenticatie alleen het ECK-ID wordt opgevraagd en teruggeven. Ook de educatieve uitgevers en distributeurs moeten zich op deze situatie aanpassen.

De Entree federatie is inmiddels volledig op deze nieuwe situatie aangepast. Dit vormt dus geen belemmering meer voor de invoering van het ECK-ID in het mbo.

3.1.4 Conclusie

Veruit de grootste inhoudelijke uitdaging ligt op het punt van de IAM-omgeving van de instellingen. Instellingen waren zelf verantwoordelijk om dit te gaan realiseren, terwijl de situatie per instelling erg verschillend is en de oplossing niet voor de hand ligt.

3.2 Aansturing

Naast het inhoudelijke vraagstuk speelt ook de aansturing van het geheel een rol.

De implementatie van het ECK-ID is georganiseerd en aangestuurd vanuit Edu-K, in de vorm van een publiek-private samenwerking (de sectorraden en brancheverenigingen van educatieve uitgevers en leveranciers). Edu-K heeft is als ketenregisseur opgetreden. Dat werkt heel goed om gezamenlijk tot afspraken en kaders te komen.

Er wordt door betrokkenen verschillend gedacht over de beste wijze van aansturing, zeker op het moment dat wordt overgegaan van een fase van beleid en kaders naar uitvoering. Voor de uitvoering is stevigere aansturing nodig en speelt ook het vraagstuk van financiering een grotere rol.

Aan de kant van de educatieve uitgevers en distributeurs wordt dit probleem gezien en is besloten om de stichting SEM (Samenwerkende Educatieve Marktpartijen) op te richten, om zo de aansturing en financiering te kunnen organiseren. Op dit moment bestaat SEM uit Noordhoff, Thieme Meulenhoff, Iddink Group, The Learning Network, Topicus en OsingadeJong.

Specifiek in het geval van de invoering van het ECK-ID is het belangrijk om op te merken dat een aantal belangrijke SIS-leveranciers hierin niet is meegenomen, en dat de leveranciers van IAM-oplossing grotendeels buiten beeld zijn.

Naast de marktpartijen is het ook nodig dat de instellingen worden aangestuurd. De verwachting bij marktpartijen is dat de MBO Raad en/of saMBO-ICT hierin een belangrijk rol spelen, maar in de praktijk maken instellingen vooral hun eigen afwegingen.

3.3 Kosten

Voor de invoering van het ECK-ID zijn geen aparte gelden vrijgemaakt. Van marktpartijen wordt verwacht dat ze op grond van de wettelijke verplichting tot dataminimalisatie en privacybescherming de nodige investeringen doen.

Marktpartijen zullen aanvullende kosten als extra investering in de kwaliteit en toekomstvastheid van hun product zien of afwentelen op de afnemende instellingen.

De scholen zullen ook behoorlijke investeringen moeten doen, grotendeels gemotiveerd met dezelfde noodzaak tot dataminimalisatie en privacybescherming.

Opvallend bij de implementatie en invoering van het ECK-ID is dat lange tijd is verondersteld dat elk van de partijen de eigen kosten zou dragen en niet zou afwentelen op de scholen. In het voorjaar van 2019 bleek echter dat de SIS-leveranciers weliswaar de koppeling met de Nummervoorziening als wettelijk verplicht (en daarmee kosteloos voor de scholen) zien, maar dat dat niet geldt voor de koppeling met de IAM-omgeving omdat daar een aparte SCIM-koppeling voor nodig is.

Een aantal instellingen is daar in het voorjaar van 2019 door verrast, temeer omdat toen ook duidelijk werd dat de investering in de IAM-omgeving groter is dan aanvankelijk wellicht gedacht. Scholen waren enerzijds extra kosten kwijt voor de SCIM-koppeling met het SIS, en anderzijds de SCIM-koppeling met de IAM-omgeving en additionele investeringen om versleuteld opslaan en doorgeven van het ECK-ID mogelijk te maken.

4. Conclusie en aanbevelingen

Dit korte onderzoek heeft tot doel te onderzoeken waarom de implementatie van het ECK-ID in het mbo zo moeizaam verloopt.

Het is uiteraard een combinatie van factoren, maar uit de gesprekken met betrokkenen blijkt dat er in de eerste plaats een aantal inhoudelijke aspecten zijn die de implementatie in het mbo aanzienlijk complexer maken dan in po en vo. Daarbij zijn de mbo-instellingen onvoldoende ondersteund en aangestuurd in de implementatie en de problemen die daarbij ontstaan. Er lijkt ook onvoldoende urgentie bij de mbo-instellingen gevoeld te worden. Tenslotte zijn de instellingen op een ongelukkig moment in het proces geconfronteerd met extra kosten.

Deze punten worden hieronder nader toegelicht

4.1 Conclusies

Inhoudelijke complexiteit

Nagenoeg alle mbo-instellingen maken gebruik van een eigen omgeving voor IAM. En deze omgeving verschilt nogal tussen instellingen onderling, zowel in de technische inrichting als in de betrokken leveranciers van producten en diensten.

Praktisch betekent dit voor mbo-instellingen dat ze niet eenvoudig een oplossing uit de markt kunnen halen. Dit wordt vooral door het volgende veroorzaakt.

- Een SCIM-koppeling tussen SIS en IAM-omgeving is geen gebruikelijk type koppeling. De meeste leveranciers van de IAM-producten bij mbo-instellingen hebben hier geen ervaring mee
- Beperkingen in de producten van Microsoft (AD, ADFS en Azure AD) zorgen ervoor dat er voor het merendeel van de instellingen geen voor de hand liggende oplossing is voor het versleuteld opslaan van het ECK-ID en het verstrekken van het ECK-ID in de keten

Aansturing en ondersteuning

Gegeven deze complexiteit bij mbo-instellingen is er te weinig aansturing en ondersteuning geweest vanuit Edu-K of andere partijen zoals saMBO-ICT of Kennisnet. Aanvankelijk is het probleem rondom IAM onderschat. IAM-leveranciers zijn onvoldoende betrokken in de gemaakte architectuurkeuzes waaronder de keuze voor SCIM, en de problematiek rondom de versleuteling van het ECK-ID.

Dit heeft er pas in een laat stadium toe geleid dat er drie scenario's zijn onderscheiden voor het gebruik van een versleuteld ECK-ID in de Microsoft omgeving, waarvan ook nog onduidelijk was op welke wijze dat precies geïmplementeerd zou moeten worden.

Iedere mbo-instelling heeft met zijn eigen leverancier(s) een oplossing moeten vinden voor de juiste inrichting van het IAM. Het heeft daarbij ontbroken aan inhoudelijke sturing en ondersteuning.

Dit heeft mogelijk te maken met de rol en positie van Edu-K, die meer een regievoerende rol heeft en geen uitvoeringsorganisatie is. Ook de MBO Raad en saMBO-ICT hebben die rol niet.

Urgentie

Daarnaast ontbreekt het bij de mbo-instellingen aan urgentie. De meeste instellingen ondersteunen de wens voor dataminimalisatie en privacy-bescherming, maar er is geen praktische noodzaak of evident voordeel te behalen.

Zowel de SIS-leveranciers als de IAM-leveranciers hebben onvoldoende vraag of druk van hun klanten ervaren, waardoor er onvoldoende voortvarend is geïmplementeerd. Dat geldt vooral voor de SIS- en IAM-leveranciers die niet direct bij Edu-K betrokken waren.

Kosten

Tenslotte zijn mbo-instellingen met meer kosten geconfronteerd dan aanvankelijk verondersteld. Voor de SCIM-koppeling tussen het SIS en de IAM-omgeving worden er in veel gevallen zowel door de SIS-leverancier als de IAM-leverancier kosten in rekening gebracht. Daarnaast hebben scholen moeten investeren in advies en implementatie van de oplossing in hun IAM-omgeving.

Samengevat blijken mbo-instelling best bereid om het ECK-ID te implementeren en daarvoor kosten te maken en inspanningen te leveren. Maar in tegenstelling tot het po en vo is de oplossing in het mbo complexer waardoor de implementatie niet relatief eenvoudig kan worden uitbesteed aan een leverancier, wat architectuurkeuzes, onderzoek, aansturing van verschillende partijen en onverwachte kosten met zich meebrengt. Als dan de urgentie al niet zo heel sterk wordt gevoeld, is het risico groot dat de implementatie wordt uitgesteld of stilgelegd.

4.2 Aanbevelingen

In het verlengde van bovenstaande conclusies worden de volgende aanbevelingen voor vervolgacties gedaan.

- Concretiseer, onderbouw en communiceer nut en noodzaak
  Zorg voor een goed onderbouwde argumentatie naar de scholen voor het doorzetten van het ECK-ID. Dit zou kunnen gaan over de juridische kant (waarom ‘moet’ het), de verantwoordelijkheid van de scholen naar de andere partijen (zoals de SIS leveranciers en andere partijen in de leermiddelenketen), de toekomstvastheid (we bereiden ons ook voor op toekomstige ontwikkelingen) of de risico’s die je loopt als je het niet doet.

- Bied gerichte en praktische ondersteuning
  Zorg ervoor dat elke mbo-instelling gericht en op maat geholpen wordt met het implementeren van het ECK-ID. Inmiddels is er voldoende ervaring opgedaan en hebben marktpartijen oplossingen gerealiseerd zodat (naar verwachting) voor elke instellingen een passende oplossing beschikbaar is.

  Omdat de situatie bij elke instelling anders is, moet elke instelling een eigen ontwerp maken en de oplossingen kiezen die daarbij passen. De praktische

ondersteuning kan eruit bestaan dat met een instelling samen een concreet ontwerp wordt gemaakt, inclusief de passende keuzes voor tools en leveranciers.

De inschatting is dat er op dit moment zoveel kennis en oplossingen beschikbaar zijn, dat elke instelling concreet geholpen kan worden.

- Ontwikkel een praktische 'toolkit'
  Om de hulp aan instellingen te kunnen bieden kan ter voorbereiding een 'toolkit' gemaakt worden, waarin is uitgewerkt in welke situatie (welk SIS, welke IAM-omgeving etc.) welke tools en oplossingen beschikbaar zijn. Op basis van die toolkit kan de gerichte hulp praktisch geleverd worden.

- Ontwikkel waar nodig nog concrete oplossingen
  Uit het onderzoekt blijkt dat er inmiddels voor elke mbo-instelling een acceptabele oplossing in de markt beschikbaar is. Mocht blijken dat dit in bepaalde situaties niet het geval is, dan kan het nodig zijn om aanvullende oplossingen te (laten) ontwikkelen.

- Heroverweeg de randvoorwaarde m.b.t. het gebruik van SCIM
  Voor het mbo is SCIM als uitgangspunt gehanteerd voor de koppeling tussen het SIS en de IAM-omgeving. De mogelijkheid om een reeds bestaand koppelvlak uit te breiden met het ECK-ID, mits beveiligd op basis van TLS 1.2 is toegestaan volgens de vereisten van de Nummervoorziening, maar wordt afgeraden en niet als mogelijke optie aan SIS leveranciers en scholen voorgesteld.

  Dit advies kan worden heroverwogen, zodat aanpassing van een bestaand koppelvlak tussen SIS en IAM-omgeving wel wordt toegestaan, mits voldoende beveiligd.

Bijlagen

Afgenomen interviews

Naam	Organisatie	Functie
Merijn van de Schoot	Onderwijsgroep Tilburg	Enterprise Architect
Marc Dietzenbacher	Vista College	Beleidsadviseur, voorzitter gebruikersgroep ECK
Chris Zintel	Kennisnet	Beleidsadviseur
Tonny Plas	Edu-K	Secretaris
Marcel Dol	Edu-K	Coördinator
Edwin Verwoerd	Iddink / Edu-K	Ketenarchitect
Marchien van Doorn	Stichting SEM	Directeur, Programma Start Schooljaar
Ben Koers	Iddink	Stichting SEM, Programma Start Schooljaar
Suzan Tessels	ROC van Amsterdam	Manager Innovatie en Integratie
Jonas de Graaff	CACI	Coördinator/specialist integratie Osiris
Michiel Nicolasen	ROC van Amsterdam	Architect technische infrastructuur
Cindy Kole	IT-Workz	Architect
Roel Griffioen	Epicenter	Architect Peoplesoft Campus Solutions

Geraadpleegde documentatie

Alleen de belangrijkste documenten worden hier genoemd.

- Edu-K, Voortgangsrapportages Programma Start Schooljaar
- KAT-advies koppeling LAS-ELO aan het Tactisch Overleg Toegang tot Leermateriaal VO/MBO van 3 april 2018
- Stichting SEM, Status update Programma Start Schooljaar, november 2020
- Kennisnet, ECK iD Voorschriften, Voorschriften voor het verwerken van het ECK iD, versie 1.0, maart 2019
- ECK iD implementatie IAM-leveranciers – overview, Informatiesessie voor IAM dienstverleners 28 februari 2019, Edwin Verwoerd

- Edu-K, Handreiking ECK-iD in Active Directory