ACEN x Odisee
DE CO-HOGESCHOOL

REFERENTIE CASE

De identitystrategie achter meer dan 12.500 studenten-accounts



Een doordacht **IGA-platform** en toekomstbestendig **identity management** voor Odisee

Over Odisee

Odisee is een Vlaamse hogeschool met **meer dan 12.500 studenten en 1.350 medewerkers,** verspreid over campussen in onder andere Aalst, Brussel, Dilbeek, Gent, Schaarbeek en Sint-Niklaas. Als lid van de **Associatie KU Leuven** faciliteert de hogeschool naast haar eigen gebruikers ook heel wat **gebruikers van KU Leuven.**

Dat brengt heel wat uitdagingen met zich mee. Studenten, docenten en externe gebruikers moeten steeds **tijdig toegang** krijgen tot de **nodige digitale omgevingen en applicaties.** En dat ook steeds met de juiste rechten.
Tijdens piekmomenten, zoals de start van een nieuw academiejaar of de aanvang van de tweede zit, moeten er **dagelijks wel tot 50 unieke identiteiten worden aangemaakt en/of gewijzigd.**

Hoe beheer je duizenden identiteiten die voortdurend veranderen? En dat terwijl één persoon tegelijk student, medewerker, gastdocent en KU Leuven-gebruiker kan zijn?

Om die processen **schaalbaar** te maken en houden, werkten Odisee en ACEN de afgelopen tien jaar samen aan een **IGA-oplossing.** Het project was geen verhaal van stilstand maar van **constante evolutie.** Tussen 2015 en 2025 evolueerde de omgeving van **Microsoft Forefront Identity Manager (FIM),** via **Microsoft Identity Manager (MIM),** naar een volledig nieuwe **midPoint**-omgeving.

Odisee
DE CO-HOGESCHOOL







DE UITDAGING

Over de jaren heen was het platform ‘out-of-shape’ geraakt en er was nood aan meer automatisatie

De samenwerking startte ruim tien jaar geleden. De **implementatie en configuratie** van een nieuw FIM-platform ligt aan de basis. De interne expert van het toenmalige platform bij Odisee was vertrokken. En daarnaast zorgde de **fusie** van HU Brussel en KaHo Sint-Lieven tot Odisee voor nieuwe noden en wensen.

De hogeschool werkte al voornamelijk met **Microsoft-technologie.** Gezien de voorgeschiedenis met FIM werd er opnieuw voor deze oplossing gekozen.

Maar die had haar limieten. Met duizenden gebruikersaccounts en een nauwere samenwerking met KU Leuven werd **identity management** steeds belangrijker. Naast studenten en medewerkers moest Odisee ook gastdocenten, consultants, tijdelijke medewerkers, werkstudenten en gebruikers met **meerdere rollen** beheren.

“Vroeger werkten we met een Excel-bestand met gebruikersnamen en wachtwoorden en werd elk account manueel opgezet. Dat is vandaag de dag simpelweg ondenkbaar, maar zo ging het wel. In de FIM-omgeving werd er veel opgevangen door custom scripts en via DevOps maar ook daar liep er vaak wel wat mis. Er was nood aan meer optimalisatie en automatisatie.”



Jan Vanneste / Operations Team Verantwoordelijke bij Odisee

Uit een recente IT-audit bleek ook dat er een probleem rond **account governance** bestond. **Externe accounts** van bv. gastdocenten werden niet structureel beheerd waardoor er zogenaamde “**ghost accounts**” ontstonden. Dat zorgde niet enkel voor onnodige licentiekosten maar vormde ook een potentieel beveiligingsrisico.

Met de samenwerking met KU Leuven werd ook steeds duidelijker dat de **kloof** tussen beide IT-omgevingen te groot was. Veel gebruikers beschikten over zowel een Odisee-account als een KU Leuven-account, elk met hun **eigen activatieproces, MFA-methode en policies.** Dat zorgde niet enkel voor verwarring bij eindgebruikers, maar maakte ook het beheer van toegangen en rechten aanzienlijk complexer.

Overgangsscenario’s zorgden er verder voor dat Odisee met haar toenmalige MIM-opstelling tegen de technische beperkingen van het platform liep.

Werkstudenten of bijvoorbeeld leraren die weer gingen studeren creëerden complexe re-hireprocessen die soms manuele actie vereisten.

Daarnaast was de **synchronisatie** tussen beide platformen ook te traag. MIM werkt op basis van geplande triggers terwijl er nood was aan een **near-real-time** flow voor gegevensuitwisseling.

Automatisatie als trigger voor meer governance

Doorheen de jaren werd het identity platform steeds verder uitgebreid met **nieuwe automatisaties en self-servicefunctionaliteiten.**

Zo werd onder andere een **Self-Service Password Reset-oplossing** geïmplementeerd waarbij gebruikers via **OTP-verificatie** (one-time password) hun wachtwoord zelfstandig konden resetten. Ook werd een portaal ontwikkeld waarmee tijdelijke gebruikers eenvoudig konden worden geregistreerd en beheerd.

Accounts worden vandaag **automatisch aangemaakt, aangepast en verwijderd** op basis van gegevens uit de verschillende bronsystemen, geconsolideerd in één centrale database. Wanneer iemand van functie, opleiding of afdeling verandert, worden de bijhorende toegangsrechten automatisch aangepast. Ook tijdelijke accounts worden gecontroleerd opgevolgd. Ongebruikte accounts worden automatisch gedeactiveerd en verwijderd.



Het gevolg? Tijdens een **optimalisatietraject** werden ongeveer **17.000 verouderde of verweesde accounts opgeschoond.**

Deze automatisaties zorgen niet alleen voor een efficiënte werking. Ze vormen ook de basis voor een **sterke governance-strategie.** Alle digitale identiteiten worden over hun volledige **levenscyclus** consistent gecontroleerd en beheerd.

De kloof tussen identiteiten

Studenten beschikten over **twee verschillende accounts** die volledig **los** stonden van elkaar én los van elkaar werden beheerd. Wanneer multifactor-authenticatie werd ingevoerd, betekende dit zelfs dat gebruikers **voor beide omgevingen een aparte authenticator-app** moesten gebruiken. Voor de studenten van Odisee was dat niet alleen verwarrend, maar ook inefficiënt.

Met het oog op een betere gebruikerservaring voor Odisee-studenten werd er ingezet op een veel nauwere **integratie** tussen beide omgevingen.

MIM werd verantwoordelijk voor het aanmaken van **Foreign Security Principals** binnen het Odisee-domein. Hierdoor konden gebruikers uit het KU Leuven-

domein eenvoudig worden toegevoegd aan **beveiligingsgroepen** en kregen zij automatisch de juiste toegangsrechten binnen de Odisee-omgeving.

Daarnaast werd het platform verder uitgebreid met geautomatiseerd beheer van rollen, teams, beveiligingsgroepen en gedeelde resources. Ook **mailboxen** en gedeelde mailboxen werden later automatisch geprovisioneerd binnen **Exchange Online.**

Ondanks die uitbreidingen werden de beperkingen van MIM steeds duidelijker. Er was meer en meer nood aan near-real-time datasynchronisatie tussen Odisee en KU Leuven. Daarnaast bleven identiteiten met verschillende hoedanigheden problemen geven. Ook **gebruikers met meerdere rollen bleven een uitdaging.** De toenmalige MIM-opstelling kon hen **geen apart AD-account** per rol geven.

De synchronisatie tussen beide omgevingen moest sneller, flexibeler en intelligenter worden. Stilaan werd er gekeken naar een nieuwe omgeving.

Waarom Odisee koos voor midPoint

Hoewel Microsoft Identity Manager jarenlang een belangrijke rol speelde, werd het platform gaandeweg steeds complexer.

Nieuwe uitzonderingen, maatwerk en bijkomende integraties maakten de omgeving steeds **moeilijker beheersbaar.** Daarnaast groeide de behoefte aan **snellere verwerking, meer transparantie en betere ondersteuning** voor gebruikers met meerdere rollen.

Samen met ACEN onderzocht Odisee verschillende opties en koos uiteindelijk voor **midPoint.**



Een belangrijk voordeel was de mogelijkheid om **verschillende persona's van één gebruiker afzonderlijk te beheren.** Studenten die ook medewerker zijn, jobstudenten of personeelsleden die opnieuw studeren krijgen elk de juiste identiteiten en rechten zonder ingewikkelde procedures.

Een doordachte architectuur en logica als fundament

Het migratieproject steunde op een sterke basis: een **goed uitgedachte architectuur.** Samen analyseerden ACEN en Odisee alle processen, koppelingen en edge cases. Bovendien werd er met een **kritische blik** gekeken naar welke zaken er wel en geen plaats hadden in de vernieuwde omgeving.

Dat leidde tot een veel **bewustere aanpak** van identity governance. Enkel processen die **voldoende meerwaarde** bieden worden geautomatiseerd. **Uitzonderingen** die disproportioneel veel complexiteit toevoegen, worden bewust anders behandeld.

> **"We denken vandaag veel kritischer na over wat in een identity management systeem thuishoort. Automatiseren is goed, maar niet wanneer je systeem onnodig ingewikkelder wordt door het toevoegen van allerlei uitzonderingen."**
>
> **Jan Vanneste** / Operations Team Verantwoordelijke bij Odisee



DE IMPLEMENTATIE

Kennisoverdracht en eenvoud als grootste troeven



> **"MIM kan soms aanvoelen als een 'zwarte doos' voor klanten. MidPoint biedt meer transparantie en voelt daardoor doorgaans beter beheersbaar en voorspelbaarder aan."**
>
> **Wouter Landuyt** / IGA-expert bij ACEN

Tijdens elke fase van het project is Odisee heel **nauw betrokken** geweest. Ontwerp, configuratie, testing en migratie werden in nauwe samenwerking uitgevoerd. Daardoor bouwde het interne team **al tijdens het project** de nodige **kennis** op rond de ins en outs van het platform. "We hebben alles samen gedaan", gaf Wim Herremans, System & cloud engineer bij Odisee, mee. "Voor ons was het belangrijk dat de kennis niet bij één persoon bleef zitten, maar intern breed werd opgebouwd."

Het **vlotte verloop van de migratie** was het resultaat van een combinatie van factoren: een sterke focus op opleiding en kennisdeling, gecombineerd met de **stabiliteit en robuustheid** van het platform. Ook uitgebreid testen speelde een belangrijke rol in het succes van de migratie. Met testomgevingen, testdatabanken en verschillende validatiefases werd de overgang zorgvuldig voorbereid voordat de uiteindelijke migratie plaatsvond.

DE RESULTATEN

Door de configuratie, eenvoud en kennisdeling voert Odisee het dagelijks beheer zelf uit.

1 Snellere verwerking van account-aanvragen

Door automatisatie wordt heel wat **manueel werk** weggenomen. Gebruikers worden automatisch aan de juiste lesgroepen gekoppeld en krijgen de correcte toegangen tot cursussen en lesmateriaal. Daarnaast kunnen gebruikers via een **self-serviceportaal** onder meer hun wachtwoord resetten. Opleidingen en diensten met veel gastgebruikers kunnen bovendien **zelf** hun **externe accounts** beheren.

2 Minder druk op de interne IT-dienst en service desk

“Er komen tot wel **90% minder identity-gerelateerde tickets** binnen tijdens drukke inschrijvingsperiodes”, vertelde Jan.

De verminderde complexiteit zorgt er verder ook voor dat er intern veel zaken kunnen worden onderzocht en opgelost.

3 Meer governance en controle

Lifecycleprocessen zorgen ervoor dat accounts worden opgevolgd. Daardoor worden verweesde accounts vermeden en blijven toegangsrechten beter afgestemd op de actuele functie of rol van een gebruiker.

Gebruikers met meerdere rollen kunnen vandaag correct worden beheerd **zonder ingewikkelde uitzonderingen of workaround-processen.**

4 Een kosten-efficiënte oplossing

MidPoint is als open-source oplossing **kosteloos.** Hierdoor is er niet alleen geen gevaar van **vendor-lock-in** maar is er ook geen extra licentiekost. Kostenefficiëntie was belangrijk omdat de hogeschool haar **budget** ook moet maximaliseren. Voor Odisee was dit ook een enorme meerwaarde.

Daarnaast kan het **interne team** het **dagelijks beheer zelf** uitvoeren en wordt ACEN enkel gecontacteerd bij grotere en/of complexere uitbreidingen aan het platform.



“Door de manier waarop we het project hebben aangepakt, was er bij Odisee al snel het vertrouwen om zelf met midPoint aan de slag te gaan.”

Wouter Landuyt / IGA-expert bij ACEN

Over de samenwerking

De evolutie tussen 2015 en 2025 is een van **continue verandering** geweest met twee vaste componenten: ACEN en Odisee samen aan de tekentafel.

Bij elke migratie of aanpassing werd er kritisch gekeken naar **problemen en noden.** Nieuwe pistes werden **samen** bekeken en onderzocht en de omgeving werd stap voor stap verder geoptimaliseerd en uitgebreid.

De combinatie van jarenlange **ervaring** met de Odisee-omgeving, **diepgaande IGA-expertise** en de rol van ACEN als **midPoint Bronze Partner** vormde een sterke basis voor een succesvolle migratie. Uitgebreide testing, een grondige voorbereiding en hands-on ondersteuning tijdens de cut-over zorgden voor een gecontroleerde en succesvolle overgang.

“Wat we zelf kunnen oplossen, nemen we met vertrouwen in handen. Voor wat we niet zelf kunnen, weten we dat ACEN maar één telefoontje verwijderd is.”

Wim Herremans / System & Cloud Engineer bij Odisee



www.acen.eu • **info@acen.eu**
Veldkant 7 - 2550 kontich België