Amsterdamse Hogeschool voor de Kunsten

Bijlage G

Visie IAM

Openbare Europese Aanbestedingsprocedure

Identity and Acces Management systeem en bijbehorende dienstverlening

IAM Architectuur

Kenmerk 15 07 22 AHK

Inhoudsopgave

1. Inleiding

1.1 Doel van dit document

Dit document beschrijft de kaders vanuit de Domein- en Enterprise-architectuur voor de aanbesteding Identity & Access management (IAM) systeem. Het is enerzijds de vertaling van de huidige opzet binnen de AHK en anderzijds de vertaling van toekomstige behoeftes die worden voorzien binnen de organisatie van de AHK.

Het document houdt daarnaast rekening met technologische ontwikkelingen binnen het IAM-domein en beschrijft de onderdelen die van belang zijn voor de AHK-organisatie en zal dit verwerken in de doelarchitectuur.

1.2 Referenties

Titel	Versie	Auteur	Vindplaats

2. Management samenvatting

2.1 Doel en positie aanbesteding Identity & Access managementsysteem

Identity & Access management is een samenstelling van technologieën en bedrijfsprocessen. Er is geen eenduidige aanpak van *identity management*, omdat er per organisatie specifieke eisen zijn, waar rekening mee gehouden moet worden. Tevens is het technologisch landschap per organisatie anders.

De volgende onderdelen geven de belangrijkste aspecten weer vanuit een business en technologisch oogpunt:

- Het voorzien van een verbeterde digitale identiteit gebaseerd op standaarden, die gebruikt kunnen worden voor het authentiseren en autoriseren van gebruikers.
- Het simplificeren van de integratie van bedrijfsapplicaties.
- Het beheren van de *Joiner, Mover* en *Leaver* (JML) processen van de organisatie.
- Ondersteunen van op internet gebaseerde applicaties voor toegang van gebruikers.

Naast het voorzien in een digitale identiteit voor verschillende soorten gebruikers en het verlenen van toegang, is het IAM-systeem een integraal onderdeel van het cyber security. Met de digitale transformatie van organisaties, is een digitale identiteit een kritisch onderdeel geworden van veel bedrijfsprocessen.

Het behandelen van het volledige IAM-proces, als een onderdeel van cyber security van AHK, is daarom van cruciaal belang, om een veilige dienstverlening te verzorgen.

2.2 Bedrijfsarchitectuur

De hogeschool AHK bestaat als opleidingsinstituut uit verschillende academies met verschillende ontstaansgeschiedenissen. AHK als koepelorganisatie voorziet de studenten, afgestudeerden, docenten en werknemers van dienstverlening, zodat elke academie hun bedrijfsvoering onafhankelijk kan uitvoeren.

Het IAM-systeem van een organisatie moet het toekomstige digitale businessmodel en eisen die door verscheidenheid van stakeholders wordt gesteld, kunnen vervullen. In het huidige tijdperk wordt digitale technologie door bedrijven veelvuldig toegepast. Binnen een organisatie zullen verschillende stakeholders vroeg of laat gebruik willen maken van deze technologie.

Daarom is het belangrijk bij deze aanbesteding, niet alleen te kijken naar de huidige rol van het IAM-systeem, maar ook naar de toekomst. Ook voor onderwijsinstellingen vindt momenteel de digitale transitie plaats. Om huidige en toekomstige behoeften te kunnen vervullen, is de keuze van het juiste systeem van cruciaal belang.

Een IAM-systeem is door Gartner gedefinieerd als "*the discipline that enables the right individuals to access the right resources at the right times for the right reasons*". Een IAM-systeem maakt het mogelijk om eenvoudig toegang te verlenen en deze te beheren tot systemen/applicaties. Microsoft Active Directory (AD) is een goed voorbeeld van 1 van de eerste voorbeelden van een IAM-systeem.

"*IAM addresses the mission-critical need to ensure appropriate access to resources across increasingly heterogeneous technology environments, and to meet increasingly rigorous compliance requirements. IAM is a crucial undertaking for any enterprise. It is increasingly business-aligned, and it requires business skills, not just technical expertise.*" (Gartner)

In de afgelopen jaren is IAM getransformeerd van een on-premise dienst, naar een Clouddienst. Traditioneel is AD gelimiteerd tot diensten op lokale en beveiligde netwerken. Maar met de komst van Clouddiensten, werden steeds meer resources buiten het netwerk van de organisatie gehost. Om IAM-diensten buiten lokale- en beveiligde netwerken mogelijk te maken, zijn nieuwe op Cloud gebaseerde diensten als Ping en Okta ontstaan. Ook heeft Microsoft een nieuwe dienst toegevoegd om dit mogelijk te maken, genaamd Microsoft Azure Active Directory (AAD).

Cloud IAM-providers (Okta, Ping, AAD) zijn Cloud IAM-providers, die het mogelijk maken om toegang tot applicaties en diensten te verlenen en te beheren die niet alleen lokaal, maar ook in de Cloud draaien.

De beperkingen van IAM-diensten worden zichtbaar als er wordt gekeken waartoe de gebruikers daadwerkelijk gerechtigd zijn. Om inzicht te krijgen in wat voor autorisatierechten gebruikers hebben, is er behoefte aan *Identity Governance and Administration* diensten.

Identity Governance and Administration (IGA) is gedefinieerd door Gartner als "*activity within the identity and access management function that concerns the governance and administration of a unique digital representation of a user, including all associated attributes and entitlements.*"

Het IGA-systeem biedt een veel meer verfijnde rechtenstructuur, die centraal beheert wat voor soort toegang gebruikers hebben in applicaties. Naast het zogenaamde *entitlement management*, controleert het IGA-systeem tevens het zogenaamde *joiner*, *mover* en *leaver* proces. Voor het creëren, wijzigen en verwijderen van digitale identiteiten is het IGA-systeem leidend.

De aanbesteding betreft het vernieuwen van het huidige IGA-systeem. Zoals aangegeven vervult momenteel Modiam deze functie. Daarnaast verwacht de AHK dat, bij het implementeren van het nieuwe IGA-systeem, dit visie document als leidraad wordt gehanteerd. Daarbij dient de doelarchitectuur die hier beschreven is nadrukkelijk aangehouden te worden als stip op de horizon en dient het nieuwe IGA-systeem in de basis te kunnen voorzien in de hier geschetste mogelijkheden.

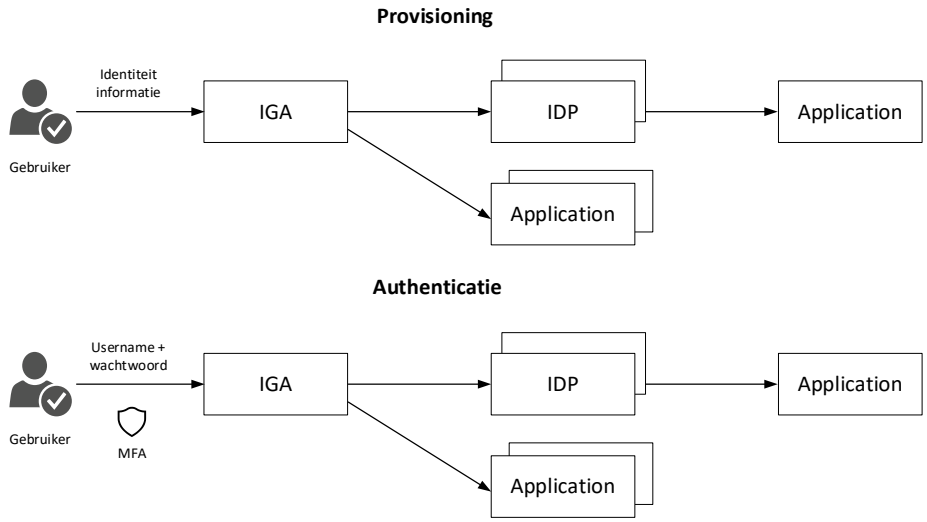
2.3 Informatiearchitectuur

Het document Bijlage F Functioneel Ontwerp Modiam IAM AHK dat deel uitmaakt van de aanbestedingsstukken, bevat de attributen die momenteel uitgelezen worden vanuit de bronsystemen en worden gebruikt voor identity provisioning naar de gekoppelde systemen. Deze attributen dienen als uitgangspunten worden gebruikt voor het JML-proces. Waar nodig zal het nieuwe IAM-systeem de lijst van attributen uitbreiden/aanpassen om de gekoppelde systemen te voeden.

Verder zal de huidige informatiearchitectuur overgenomen worden in het nieuwe platform en waar nodig worden aangepast. Het primaire uitgangspunt is dat alle bestaande processen intact blijven bij het vernieuwen van het IGA-systeem. Tegelijkertijd zal bij het implementeren van het nieuwe IGA-systeem de basis gezet worden voor een transitie architectuur, als een tussenstap naar de target architectuur.

2.4 Impact op de technische architectuur

Het huidige IGA-systeem Modiam is gebaseerd op een architectuur, waarbij alle authenticatie en autorisatie processen altijd door Modiam lopen. Ook worden alle identiteiten door Modiam gecreëerd. Het volgende plaatje geeft een vereenvoudigde versie van deze huidige architectuur weer:



Figuur 1. Huidige IAM-proces

Modiam wordt naast voor *provisioning* en authenticatie, ook als *user-directory* en voor *Multi-Factor Authentication (MFA)* gebruikt. Dit maakt Modiam niet alleen een kritisch onderdeel van het AHK IT landschap voor IGA-processen, maar ook van dagelijkse operationele processen. Hierdoor dient het platform te voldoen aan hoge eisen voor de beschikbaarheid en stabiliteit. Dat is momenteel niet het geval, wat zeer regelmatig operationele problemen veroorzaakt.

3. Doel en positie IAM Visie AHK

3.1 Inleiding

Het bestuur van de AHK heeft besloten om het bestaande IGA-systeem van de AHK te vernieuwen. De reden hiervoor is voornamelijk de status van het platform. Het huidige platform, is complex, lastig aanpasbaar en niet betrouwbaar gebleken. Het vernieuwde platform dient deze gebreken op te lossen en nieuwe technologieën voor de komende jaren te ondersteunen. Het doel is om een stabiel, betrouwbaar, flexibel en gebruikersvriendelijk platform te creëren, die het AHK voor de komende jaren kan gebruiken.

3.2 Doel

Dit document heeft twee doelen. Ten eerste beschrijft het de kaders en de richtlijnen voor de IGA-aanbesteding. Partijen die willen inschrijven op de aanbesteding kunnen het document gebruiken als richtlijn voor de toekomstige visie die AHK heeft omtrent IAM-architectuur. Het beschrijft de kaders waarbinnen de implementatiepartner dient te opereren en de oplossing moet realiseren.

Tegelijkertijd beschrijft dit document, de toekomstige IAM *roadmap* voor de gehele AHK. De aanbesteding zal een deel van deze architectuur vervullen. Toekomstige aanpassingen dienen in lijn met deze architectuur uitgevoerd worden en de richtlijnen dienen in acht te worden genomen.

3.3 Projectorganisatie

Bij het organiseren en begeleiden van het aanbesteding traject zijn de volgende projectleden betrokken:

- Job Rodenburg, manager IT Operations en projectmanager
- Mirjam Kloosterman, Senior inkoper en Duurzaamheidscoördinator
- Rob Dörr, Specialist Infrastructuur services
- John Bos, Specialist applicatie- en gegevensservices
- Ali Simsek, IAM Consultant en Security Architect

Verder heeft het projectteam de verantwoordelijkheid, om de faculteiten bij het aanbesteding traject te betrekken en hun behoeften die relevant zijn binnen het IAM-domein mee te nemen in de aanbesteding.

3.4 Betrokken Architecten

Vanuit de AHK-organisatie zijn geen directe architecten betrokken. Alleen Ali Simsek is betrokken als IAM-consultant bij het begeleiden en ondersteunen van het aanbesteding traject. Tevens acteert Ali als IAM/Security architect, om de toekomstige IAM Visie van de AHK te definiëren. De toepassing en het uitdragen van de IAM Visie wordt verankerd binnen de IM- en ICT-afdeling.

3.5 Bedrijfsdrijfveren

De primaire bedrijfsdrijfveer voor het vernieuwen van het IGA-systeem is, zoals reeds eerder aangegeven stabiliteit, betrouwbaarheid, flexibiliteit en gebruiksvriendelijkheid.

3.6 Architectuurdrijfveren

Vanuit de architectuur gezien, dient het nieuwe IGA-systeem veilige autorisatie en authenticatie mogelijkheden te bieden. Dit geld niet alleen voor de bestaande systemen en de *on-premise* omgeving, maar ook voor de clouddiensten waar AHK steeds vaker gebruik van maakt.

Verder zullen de architectuurontwerpen zich voornamelijk richten op de gebruiker, het apparaat en de verhouding die zij hebben tot applicatie en data.

4. Bedrijfsarchitectuur Aanbesteding Identity & Access managementsysteem

4.1 Inleiding

Een positieve gebruikerservaring tezamen met een veilige en stabiele IAM-omgeving, zorgen voor een positieve beoordeling van een organisatie, wat zich weer reflecteert in een verbeterd bedrijfsresultaat[1]. Om een dergelijke ervaring te kunnen bieden, moet er in technologie, systemen en processen geïnvesteerd worden. IAM is een technologie die dit mogelijk kan maken. Het is voor elke organisatie de voordeur en elke gebruiker komt met deze technologie in aanraking.

Een moderne applicatie die gebruiksvriendelijk is, zal toch een zeer negatieve impact op de eindgebruiker hebben, wanneer het inlogproces niet juist functioneert. Het toekomstige IAM-systeem van de AHK, moet in de volgende cruciale behoeftes voorzien:

- **Beheer van identiteiten (medewerkers, studenten en gasten), voorkeuren en profielen voor alle toegangskanalen en apparaten**

  Gebruikers verwachten een helder, eenduidig en veilig authenticatieproces bij alle diensten die de AHK biedt. Dit kan alleen gerealiseerd worden als er een nauwkeurig JML-proces geïmplementeerd is. Daarnaast is het belangrijk dat er zoveel mogelijk gebruik wordt gemaakt van *“selfservice”* processen. Deze processen maken het makkelijk om veel aanvragen geautomatiseerd zelf af te handelen, zonder het operationele team te belasten. Ook is de afhandeltijd van dit soort processen veel sneller, in vergelijking met aanvraag/goedkeur processen.

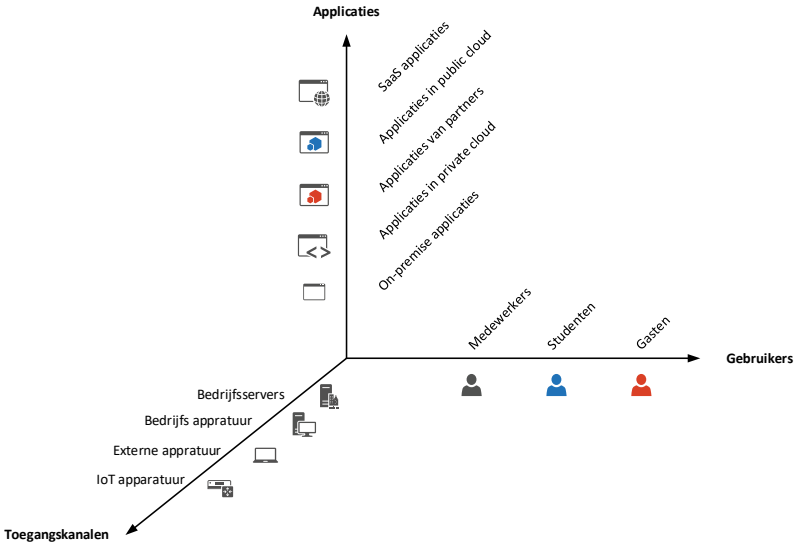
- **Beheer van gegevens en privacy-voorkeuren door de gehele Enterprise**

  Digitale identiteit is onherroepelijk gekoppeld aan informatie en vooral privacygevoelige informatie. De informatie is belangrijk voor het juist authentiseren en autoriseren van gebruikers en om de veiligheid van informatiesystemen te waarborgen. Het gebruiken, vastleggen en distribueren van *Personally Identifiable Information (PII)* moet door het IAM-systeem gewaarborgd worden en voldoen aan algemene voorschriften zoals het *General Data Protecting Regulation (GDPR)*. De gegevens die gebruikers invoeren moeten centraal vastgelegd en beheerd worden en hun privacy-voorkeuren gehonoreerd worden.

Het is van cruciaal belang om gebruikerservaring mee te nemen in de afweging voor de juiste architectuur voor het nieuwe IGA-systeem. Daarom is er ook besloten om alvorens het aanbesteding traject in te gaan, een AHK specifieke IAM Visie te ontwikkelen. De visie zal ontwikkeld worden op basis van de volgende afwegingen:

- Het huidige IAM-landschap en de rol die het vervult
- De gebruikerservaring en behoefte
- De wensen/eisen van de stakeholders/faculteiten
- De middelen die AHK beschikbaar heeft en wil investeren in het IAM-systeem. Denk hierbij aan mensen, hardware, geld en tijd.
- De toekomstige ontwikkelingen in het IAM-domein

Het onderstaande figuur, illustreert het raakvlak waarbinnen het IAM-domein opereert. Het toont de invloed van verschillende typen gebruikers (medewerkers, studenten, gasten) en hun interactie met verschillende applicaties. Denk hierbij aan moderne applicaties die in een *cloud* omgeving draaien, zoals Office 365. Maar je kunt ook denken aan applicaties die op het interne netwerk van de AHK draaien, zoals een Exact applicatie die buiten het netwerk van de AHK niet bereikbaar is. Als derde dimensie zijn de toegangskanalen belangrijk. Deze kunnen binnen de organisatie in diverse vormen aanwezig zijn, van AHK-servers die ook weer op het interne netwerk van de AHK staan, tot werklaptops van medewerkers, tot mobiele telefoons van studenten, tot kaartlezers van gebouwbeheersystemen.

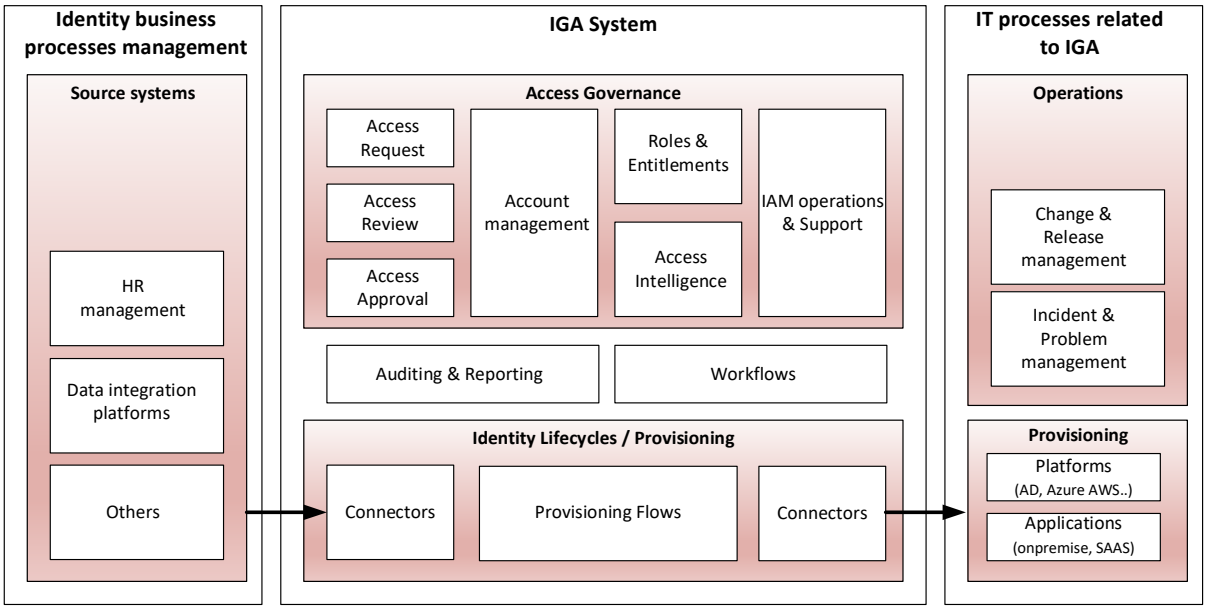


Figuur 2. IAM-systeem met relatie tot applicatielandscape, gebruikers en toegangskanalen

Er is een correlatie aanwezig, tussen wie toegang heeft op welke applicatie via welk kanaal. De architectuur visie voor de AHK moet de juiste toegang op elk toegangskanaal (apparaat) op elke interne of externe applicatie geven, voor medewerkers, studenten en gasten.

4.2 Producten/diensten

Het Identity & Access managementsysteem heeft als primaire verantwoordelijkheid het *identity lifecyle management.* Het zogenaamde *Joiner, Mover and Leaver* process. Het volgende overzicht geeft de capabilities van een IGA-systeem weer en de afhankelijkheden naar andere systemen:



Figuur 3. IGA-systeem in relatie tot applicatielandschap, gebruikers en toegangskanalen

Identiteit-bronsystemen dienen als input voor het IGA-systeem. Het IGA-systeem gebruikt de bron informatie voor:

- *Access Governance*: Dit onderdeel van het IGA-systeem voorziet in de toegangsbeheer functionaliteit. Daarnaast biedt het mogelijkheden voor het operationeel beheren van het systeem.

    Access Request, Review en Approval: Gebruikers die toegang willen krijgen, kunnen met behulp van een *self service request*, zelf een aanvraag indienen. Gebruikers dienen een aanvraag in voor een specifieke applicatie, waarna een proces wordt gestart. De bevoegde persoon ontvangt een notificatie van de aanvraag en kan dan de aanvraag beoordelen en eventueel goedkeuren.

    Accountmanagement: Het beheer van de account. Afhankelijk van de situatie in het bronsysteem of operationeel worden accountstatus of rechten veranderd in het IGA-systeem en/of in de applicaties/platforms.

    Roles & Entitlement: Een identiteit krijgt vanuit de *Joiner* flow één of meerdere rollen toegekend. Dit gebeurt op basis van de informatie afkomstig vanuit de bronsystemen. Dit zogenaamde *birthright* is het initiële rol die iemand krijgt. Aan een rol zijn rechten verbonden en op basis van een rol worden de vooraf gedefinieerde rechten aan de persoon toegekend. Tijdens de *lifecycle* van een identiteit, kunnen meerdere rollen aan een identiteit toegekend of verwijderd worden. Afhankelijk van het autorisatie model kan ook onafhankelijk van en rol, rechten (*entitlements*) aan een identiteit toegekend worden.

    Access Intelligence: Dit is het proces, waarbij informatie met betrekking tot de identiteit en toegang wordt verzameld en vervolgens wordt gebruikt om keuzes te maken in het autorisatieproces. Een voorbeeld hiervan is de Multi-factor Authenticatie (MFA) eis. Wanneer gebruikers regelmatig op hetzelfde tijdstip vanuit hetzelfde IP-adres inloggen kan van een MFA worden afgezien.

    IAM Operations & Support: Dit zijn de operationele werkzaamheden, die uitgevoerd moeten worden bij normaal functioneren van het systeem.

- *Identity Lifecycles / Provisioning* : Dit onderdeel van het IGA systeem bepaalt aan de hand van de informatie afkomstig vanuit het bronsysteem, welke identiteiten gecreëerd moeten worden in applicaties en platformen.

    Connectors: Dit zijn de voorzieningen die standaard aanwezig zijn in een IGA-systeem om een integratie te realiseren. Zowel naar de bronsystemen als naar de target systemen zijn connectoren nodig. Vanwege de diversiteit van applicaties waarmee integratie gerealiseerd kan worden, is het aannemelijk dat er niet altijd een standaard connector aanwezig is. In dat geval, wordt een connector *custom* aangemaakt.

    Provisioning Flows: De logica voor het bepalen welke identiteit in welke applicatie/platform gecreëerd, moet worden is geïmplementeerd in *Provisioning Flow*.

- *Operations:* Het proces van inloggen is een belangrijk onderdeel voor bedrijfsprocessen die stabiel en betrouwbaar moet zijn. Omdat het cruciaal is dat gebruikers te allen tijde de mogelijkheid moeten hebben om in te loggen, zijn operationele en ondersteunende activiteiten cruciaal. De gegevens in kunnen zien en de benodigde functionele mogelijkheden zijn ook een onderdeel van het IGA-systeem. Daarnaast bevat het operationele proces *change & releasemanagement*. Hiermee worden wijzigingen aan het IGA-systeem gefaciliteerd.

- *Provisioning*: Het *provisioning* onderdeel is het creëren van identiteiten. Waar voorheen identiteiten rechtstreeks in applicaties werden gecreëerd, worden in moderne platformen Identity Providers (IdP) gebruikt. Identiteiten worden alleen maar in IdP's gecreëerd en applicaties worden geonboard op IdP's en krijgen identiteitsinformatie op basis van *single-sign-on*.

4.2.1 Afbakening

Zoals in figuur 2 weergegeven zijn identiteiten, applicaties en toegangskanalen een belangrijk onderdeel van de doelarchitectuur van de AHK. Alle onderdelen moeten op elkaar afgestemd zijn voor het bereiken van de gewenste doelen. Dit document is afgebakend tot het IAM-systeem met afhankelijkheid naar het applicatie en toegangskanalen. De benodigde aanpassingen en afhankelijkheden zullen daarom gelimiteerd zijn tot IAM. De applicaties en toegangskanalen (BYOD, werkplekken, servers, mobiele telefoons) worden buiten beschouwing gelaten voor deze aanbesteding.

4.2.2 Beleidslijnen, richtlijnen, standaarden

Er zijn momenteel geen beleidslijnen, richtlijnen en standaarden bekend, waarmee in dit document rekening mee is gehouden.

5. Informatiearchitectuur Identity and Access management

5.1 Inleiding

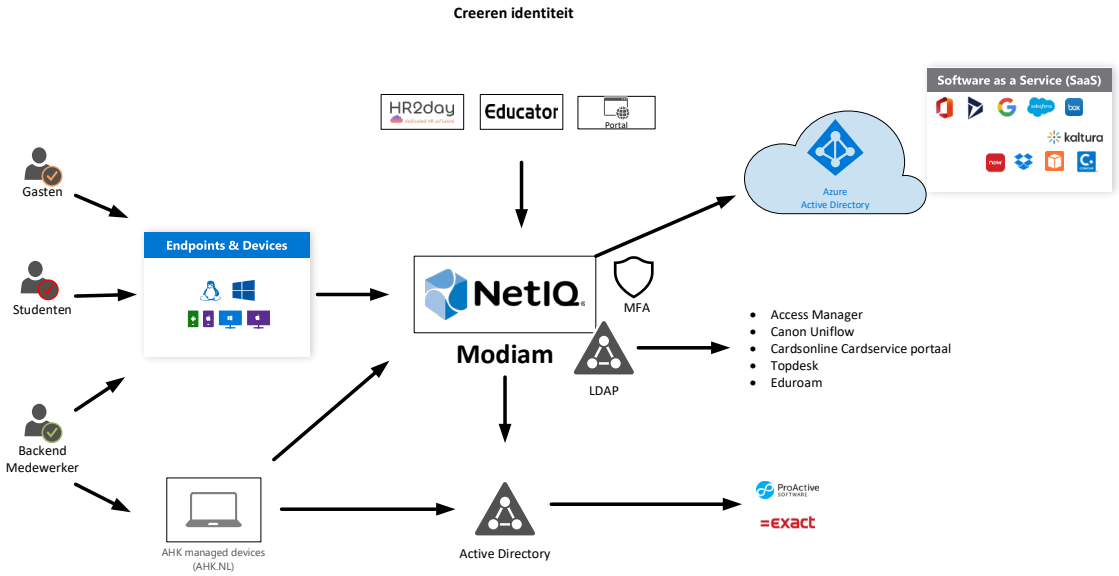
Het huidige landschap van de AHK heeft 3 componenten, die samen het IAM-platform vormen:

- Modiam, een *custom* implementatie van het NetIQ product van MicroFocus.
- Microsoft Active Directory (AD)
- Microsoft Azure Active Directory (AAD)

Deze componenten zijn met een specifiek doel aangeschaft. Voor de toekomstige architectuur, is het vernieuwen van Modiam in scope. AD en AAD zullen blijven bestaan en dienen op een juiste manier ingezet te worden en dienen als basis voor de toekomstige architectuur. De toekomstige architectuur, zal zich focussen op het *enablen* van de behoeftes van de AHK en tegelijk zo dicht mogelijk bij de referentie architectuur van Microsoft blijven. Dit is een onderdeel van de toekomstvisie van de AHK, meer standaardisatie en zo min mogelijk aanpassingen.

5.2 Huidige IGA-applicatiearchitectuur

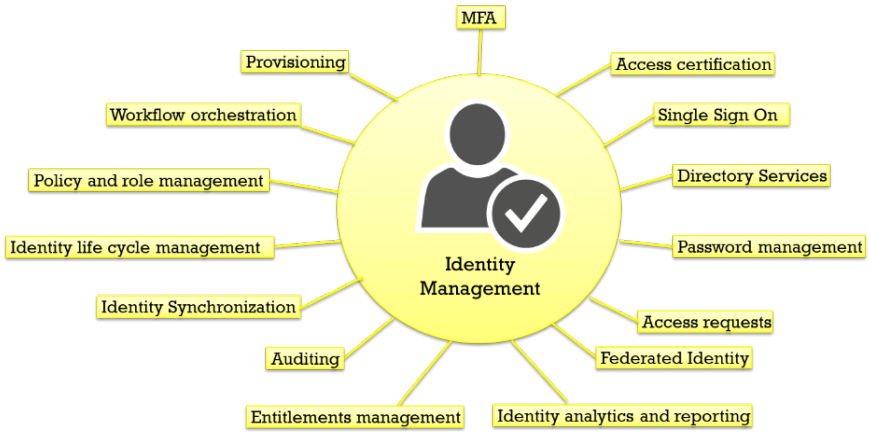
Het Modiam systeem dient als IGA-platform en de AD en AAD dienen als Identity providers. HR2day en Educator zijn als bronsysteem gekoppeld aan Modiam. Op basis van de JML-logica geïmplementeerd in Modiam, worden identiteiten rechtstreeks gecreëerd in AD, AAD en *target* applicaties. De volgende figuur geeft deze relaties weer:



Figuur 4. Huidige IAM-applicatiearchitectuur

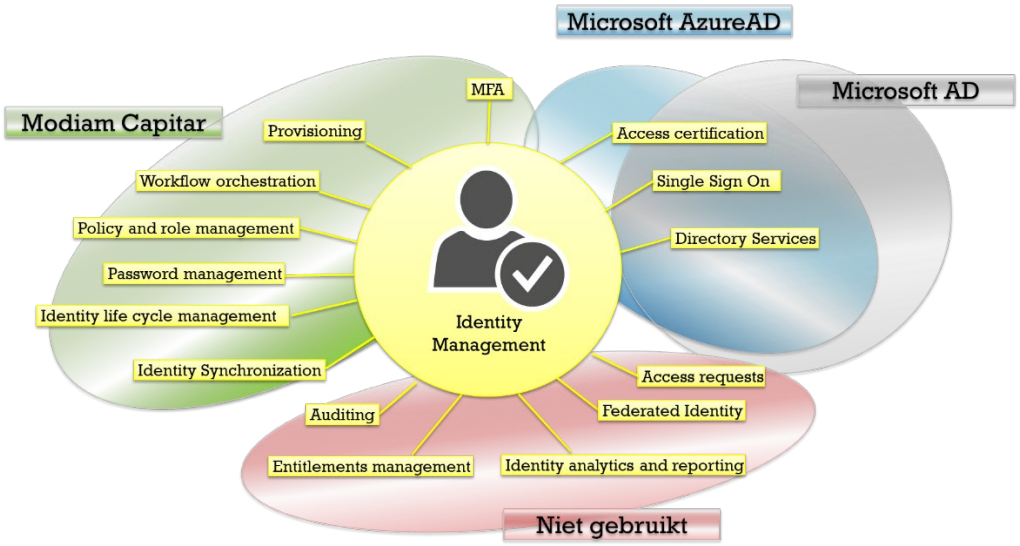
Zoals weergegeven in het bovenstaande plaatje, staat Modiam centraal in het IAM-platform. Het voorziet niet alleen in *provisioning*, maar ook in authenticatie, MFA, identiteit correlatie en *user directory* functionaliteiten.

In figuur 3 is er een overzicht gepresenteerd van functies in relatie tot de organisatie en andere systemen. Als we nu vanuit het perspectief van een gebruiker kijken, een zogenaamde *user-centric* benadering, dan krijgen we onderstaande figuur:



Figuur 5. IAM-functies

De functies vormen de basis van elk IAM-systeem. Omdat de AHK-architectuur meerdere IAM-componenten bevat met overlappende IAM-functionaliteit, gaan we eerst analyseren hoe deze momenteel zijn ingezet. Figuur 6 geeft een overzicht van de verdeling van de IAM-functies weer. Hierbij moet er rekening mee worden gehouden, dat deze verdeling alleen op hoofdlijnen wordt geïllustreerd. Specifieke onderdelen kunnen afwijken van het weergegeven overzicht.



Figuur 6. IAM-functies verdeling

Figuur 6 illustreert, hoe verschillende componenten momenteel worden ingezet. Behalve het feit, dat het Modiam platform veel functies vervult binnen de huidige architectuur, valt ook de relatief beperkte rol op die AD en AAD hierbinnen hebben. Daarnaast zijn er belangrijke functies die nog helemaal niet gebruikt worden.

Traditioneel hebben veel organisaties een eigen AD, een centraal systeem waarin het gebruikersbeheer van groep *policies*, werkplekbeheer, authenticatie en autorisatie samenkomen. Zo heeft ook de AHK een AD, waar iedere medewerker een identiteit in krijgt.

Anders dan bij medewerkers, krijgen studenten geen AD account. Studenten krijgen alleen in AAD een identiteit, om zo toegang te krijgen tot de clouddiensten van AHK. De AHK heeft geen bewuste keuze gemaakt voor AAD. AAD is gekoppeld aan de M365-dienst van Microsoft en kan met het huidige licentiemodel van de AHK, zonder additionele kosten gebruikt worden.

Net als studenten, zijn er ook binnen de AHK medewerkers die geen laptop krijgen, maar die wel een AD-identiteit hebben, omdat ze van het type “medewerker” zijn. Omdat ze geen laptop hebben, kunnen ze niet bij de *on-premise* applicaties van AHK. Een AD identiteit is hierdoor nutteloos.

Het Modiam platform verzorgt momenteel ook de correlatie tussen AD en AAD. Volgens de referentiearchitectuur van Microsoft, moet dit uitgevoerd worden met AADConnect, om een volledig hybride werkomgeving te creëren voor de medewerkers met een laptop. Omdat dit momenteel *custom* is geïmplementeerd in Modiam, is er geen correlatie van identiteiten. Het gevolg is dat bepaalde clouddiensten niet gebruikt kunnen worden, hoewel ze wel zijn aangeschaft door de AHK. De MFA-functionaliteit is hier een mooi voorbeeld van. De afwijkende implementatie ten opzichte van de referentiearchitectuur introduceert niet alleen additionele kosten, het geeft ook een negatieve gebruikerservaring. Tevens introduceert het nieuwe veiligheidsrisico’s, doordat gebruikers meerdere keren in verschillende applicaties moet inloggen.

6. De nieuwe rol van het IGA en de doelarchitectuur

6.1 Inleiding

Kijkend naar de wensen/eisen van de AHK, zal de doelarchitectuur drastisch veranderen. De werkwijze van organisaties, zo ook van de AHK is in de afgelopen jaren veranderd. Medewerkers en studenten hebben de behoefte, om vanuit verschillende plekken, met verschillende apparaten de applicaties die de AHK aanbiedt, te kunnen benaderen.

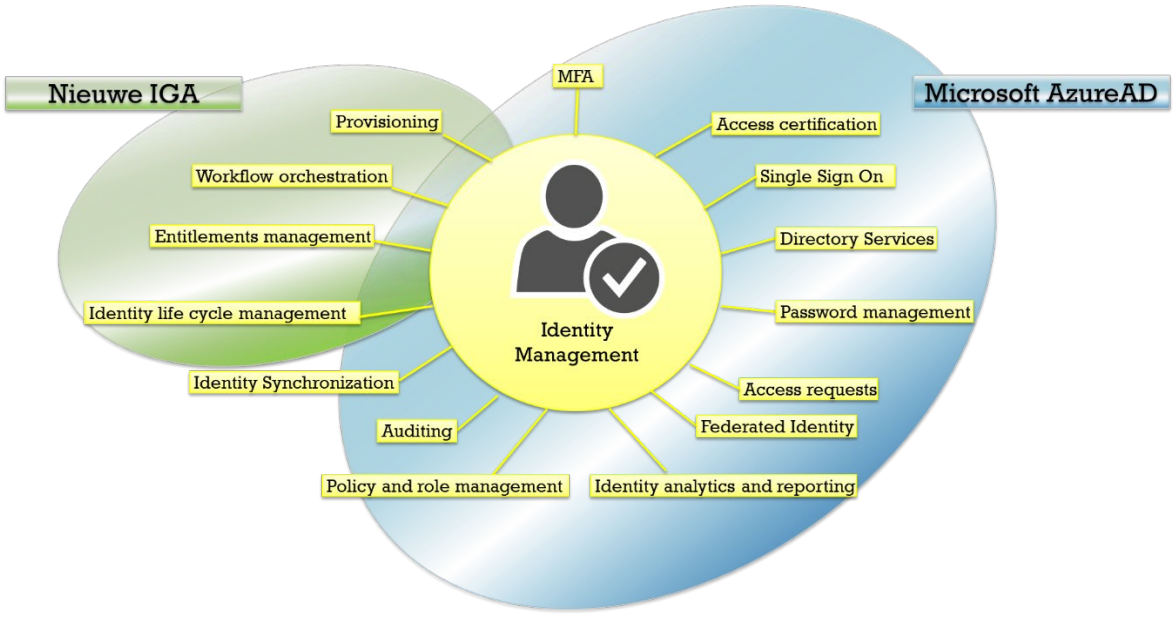
Daarnaast is er behoefte om onderscheid te maken tussen verschillende docenten (vast, tijdelijk, inval) en deze ook van een ander type digitale identiteit te voorzien. Hierdoor kan bijvoorbeeld het *onboarding* proces versneld worden voor inval-docenten, maar hun rechten en mogelijkheden beperken.

6.2 Doel IGA-applicatiearchitectuur

In de doelarchitectuur van de AHK, speelt AAD een veel prominentere rol. Het zal de primaire IDP zijn, voor de digitale identiteiten van AHK. Applicaties zullen op AAD *geonboard* worden. Ook zal in de toekomst, werkplekbeheer vanuit Intune uitgevoerd worden. Intune is vernieuwde Cloud werkplekoplossing van Microsoft. De integratie van Intune met AAD zal het benodigde apparaat (Windows, Mac, Android) onafhankelijkheid realiseren voor AHK. AAD zal onafhankelijk vanuit welk apparaat een gebruiker inlogt, gebruikers valideren (*conditional access)* op hun rechten en toegang verlenen. AD zal tijdens de transitiefase nog aanwezig zijn, maar zo min mogelijk worden ingezet.

Daarom zal er ook nog steeds gebruikt worden gemaakt van AADConnect om de correlatie van AD naar AAD te regelen. Deze zal bestaan, zolang nog behoefte is aan een AD. Vanuit het IGA-platform, zullen identiteiten alleen naar AD *geprovisioned* worden. AADConnect zal de identiteiten in AAD aanmaken, met de informatie vanuit AD.

Zaken als passwordmanagement, MFA en alle andere diensten gerelateerd aan IAM en security zullen zover mogelijk, op AAD plaatsvinden. Verder zal een *key* functionaliteit als *Identity Federation* ingezet kunnen worden, om aan business partners en gastdocenten toegang te kunnen verlenen met hun eigen identiteit. De rolverdeling binnen de nieuwe IAM-functie in de doelarchitectuur ziet er als volgt uit:

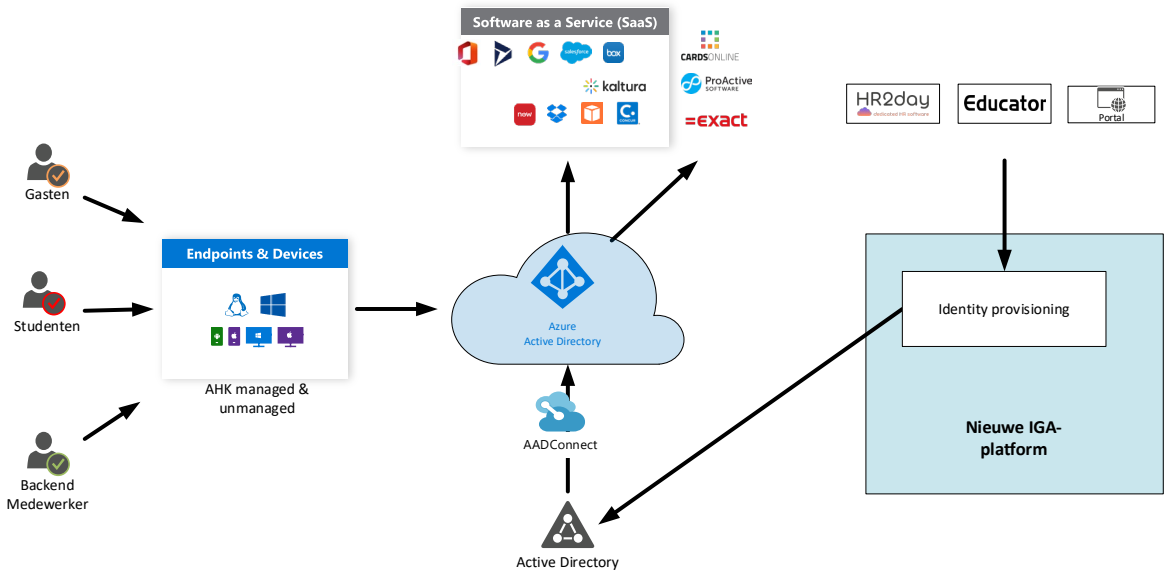


Figuur 7. IAM-functies verdeling

Door de IAM-functies op deze manier te verdelen, zal het IAM-landschap voorbereid worden op een *Zero-Trust* gebaseerde Enterprise Architectuur. AHK gaat de principes van *The Open Group* hanteren om tot een Zero-Trust architectuur te komen. Kort opgesomd, omvatten de *Zero-Trust commandments van The Open Group* het volgende (voor de authenticiteit is het Engels overgenomen):

1. Validate Trust Explicitly: Security assurance shall rely on explicitly validating trust decisions using all relevant available information and telemetry.
2. Enable Modern Work: Security discipline shall enable productivity and manage risk as the organizational capabilities; goals, environment, and infrastructure continuously evolve.
3. Enable Pervasive Security: Security discipline shall be integrated into the culture, norms, and processes throughout the organization.
4. Secure Assets by Value: Security controls shall be designed to protect business assets appropriate to their business value and expected risk.
5. Implement Asset-Centric Controls: Asset-specific security controls (versus broad infrastructure controls) shall be implemented whenever available to minimize disruption of productivity and increase precision of security/business visibility.
6. Enable Simple and Sustainable Security: Security controls shall be as simple as possible while remaining practicable, scalable, and sustainable for the full lifecycle of the business asset.
7. Utilize Least Privilege: Access to systems and data shall be provided only as required, and access shall be removed when no longer required.
8. Improve Continuously: Security teams shall continuously evolve and improve to remain successful in an environment that constantly changes.
9. Make Informed Decisions: Security teams shall make informed decisions based on the best information that can be made available.

Een modern IDP zoals AAD ondersteunt en voorziet in de benodigde functionaliteit, om de bovenstaande principes te kunnen implementeren. Uitgaand van het bovengenoemde zal het beoogde IAM-landschap van AHK, er als volgt uit zien:



Figuur 8. Target IAM-applicatiearchitectuur

Binnen de doelarchitectuur werken gebruikers vanuit de Cloud, wat een groot gedeelte van de wensen van AHK zal vervullen. Verder laat het overzicht nog steeds een AD zien. Zoals eerder vermeld, zal deze blijven bestaand zolang dit nodig is.

Het overzicht laat het *identity provisioning flow* zien. Er zal wel degelijk integratie, tussen het nieuwe IGA-platform en AAD aanwezig zijn, deze zal alleen voor *entitlement* worden gebruikt. Zodra AD verwijderd wordt, zal de *provisioning* rechtstreeks in AAD uitgevoerd worden.

Het IGA-platform is primair verantwoordelijk voor het creëren van identiteiten in de IDP's en niet in de eind-applicaties. Hierop kan een uitzondering gemaakt worden, tijdens de transitiefase en voor applicaties die de moderne protocollen niet ondersteunen. Dit zal als uitzondering behandeld moeten worden. Uiteindelijk is het de bedoeling dat applicaties één van de volgende protocollen moeten ondersteunen voor SSO:

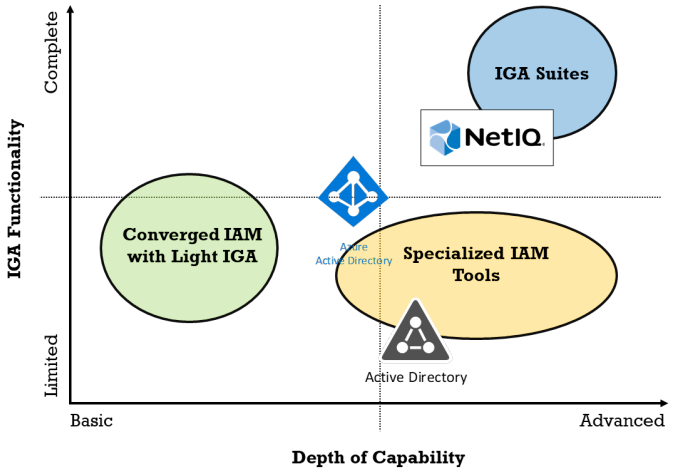
- **SAML** (Security Assertion Markup Language) is een open federatie standaard die bedoeld is om gebruikers in te laten loggen op een IdP en waarbij de applicatie de authenticatie token gebruikt, om de gebruiker toegang te verlenen.
- **SCIM** (System for Cross-Domain identity Management) is een open standaard om identiteiten te creëren in verschillende domeinen. In tegenstelling tot SAML, is SCIM ontworpen om identiteit te synchroniseren. Maar SCIM kan ook gebruikt worden voor SSO net als SAML.
- **OAuth 2.0** (Open Authorization) is een open standaard die gebruikt wordt voor delegatie van toegang. Net als bij SAML, wordt de gebruiker gedelegeerd naar een IdP om in te loggen. Vervolgens wordt een *access token* gegenereerd, die door een applicatie gebruikt kan worden om toegang te verlenen.
- **OpenID Connect** is een uitbreiding op OAuth 2.0 waarbij niet alleen een access token gegenereerd wordt, maar ook een *id token* met gebruikersinformatie. De gebruikersinformatie kan gebruikt worden door de applicatie.

OpenID Connect is het uiteindelijk beoogde protocol voor de AHK. Op termijn zouden alle applicaties OpenID Connect moeten ondersteunen. Tevens zou bij de aanschaf van applicaties de ondersteuning van OpenID Connect als *knock-out* criterium moeten gelden vanuit architectuur oogpunt.

6.3 Nieuwe IGA-platform voor AHK

De rol van het nieuwe IGA-platform zal gecentraliseerd worden en gereduceerd tot het creëren en beheren van identiteiten, het beheren van rechten en workflow orkestratie. Kijkend naar de verschillende vormen van IAM-systemen, zijn er diverse systemen met verschillende functionele eigenschappen. Door een duidelijke rol en verantwoordelijkheid aan het IGA-systeem toe te kennen, kan de AHK op basis van de gewenste functies het juiste nieuwe IGA-platform selecteren.

Het volgende overzicht geeft de verschillen in een grafiek weer:



Figuur 9. IAM-tools (Gartner ID G00734125)

Het overzicht, afkomstig van Gartner onderscheidt *IGA Suites*, *Specialized IAM tools* en *Light IGA tools*. Daarbovenop zijn de huidige tools die de AHK heeft geplot.

De *IGA Suites* zijn de meest uitgebreide platformen met een grote diversiteit aan functionaliteit. *Specialized IAM-tools* zijn daarentegen zeer beperkt in de functies die ze aanbieden, maar deze functies zijn wel heel erg uitgebreid. Een derde optie en relatief nieuw, zijn de zogenaamde *Light IGA* tools. Deze zijn relatief goedkoop, eenvoudig te implementeren, maar bieden alleen de hoognodige *core* IAM-functionaliteiten aan.

7. Niet-functionele eisen

Stabiliteit

Het systeem kan gedurende lange tijd stabiel en zonder enige interrupties actief zijn. Mocht het systeem door een onverwachte situatie inactief zijn, dan dient het mechanisme van authenticatie niet beïnvloed te worden door het IGA-systeem.

Flexibiliteit

Het systeem is in staat om de specifieke eisen met betrekking tot de Joiner, Mover en Leaver te ondersteunen en waar nodig specifieke uitzonderingen in het systeem op te nemen.

Veiligheid

Het systeem waarborgt in alle situaties de gegevens die het systeem bevat en voorziet in mechanismes om fatsoenlijk gebruikersbeheer en systeembeheer toe te passen. De informatie die het systeem bevat, kan onder geen beding ongeautoriseerd benaderd worden.

Integratie

Het systeem ondersteunt het integreren van zowel de bestaande *on-premise* omgevingen, alsmede de moderne Cloudomgevingen van AHK.

Architectuur (doel)

Het systeem ondersteunt deze AHK IAM Visie, waarbij het een onderdeel vormt van het complete IAM-landschap van de AHK. Als *identity provider* is AAD geïdentificeerd, het systeem zal voornamelijk de rol van *identitiy provisioning* en *identity entitlement* functionaliteit op zich nemen.

Architectuur (transitie)

Vanwege de diversiteit van applicaties, moet het systeem in staat zijn om bestaande *legacy* applicaties te blijven ondersteunen. Het implementeren van de doelarchitectuur zal tijd nodig hebben. Het systeem moet moderne en voornamelijk op SaaS gebaseerde applicaties, maar ook bestaande *on-premise legacy* applicaties ondersteunen.

8. Vast te stellen aanbevelingen

De aanbevelingen vanuit architectuur zijn om bij de IGA-aanbesteding niet naar de beste en meest uitgebreide leverancier te kijken, maar naar een leverancier die het juiste IGA-product heeft dat de behoeftes van de AHK afdekt. Met juist bedoelen we in deze context *just enough*. Zoals weergegeven in figuur 9, zal een *Light IGA* de kosten reduceren en minder complex zijn om te implementeren.

De organisatie zal er wel rekening mee moeten houden, dat versneld naar de doelarchitectuur moet transformeren. Het ondersteunen van SSO en moderne protocollen zal het doel moeten zijn.

Tegelijkertijd moeten bestaande applicaties zoveel mogelijk gemigreerd worden naar AAD om consistentie en eenvoud te bereiken.