PROJECT START ARCHITECTUUR_

IDM / IAM

Status definitief

Auteurs:

Dennis Ortsen (Solution Architect)

Marco de Haan (Solution Architect)

23 november 2020

HAN_UNIVERSITY OF APPLIED SCIENCES

VERSIENR	DATUM	AUTEUR	WIJZIGING
0.1 – 0.5	18-09-2020 – 01-20-2020	DENNIS ORTSEN	EERSTE OPZET, DOEL SCOPE MIDDELS APDRA, AFHANKELIJKHEDEN, STANDAARDEN, INFORMATIEKADERS
0.6	13-10-2020	DENNIS ORTSEN	HERSTRUCTURERING INHOUD T.B.V. DUIDING OPBOUW
0.7	16-10-2020	DENNIS ORTSEN	INFORMATIE- EN INFORMATIESYSTEEMKADERS
0.8	05-11-2020	DENNIS ORTSEN	HUIDIGE ARCHITECTUUR, FEEDBACK MARC DE GOEIJ EN MARCO DE HAAN VERWERKT
0.9	12-11-2020	DENNIS ORTSEN MARCO DE HAAN	FEEDBACK EDWIN CASTELEIN VERWERKT, GEBRUIKTE BEGRIPPEN, HERSTRUCTURERING INHOUD
1.0	23-11-2020	DENNIS ORTSEN MARCO DE HAAN	FEEDBACK EDWIN CASTELEIN, WESLEY CORNELISSEN, JAN OVINK VERWERKT

Tabel 1: wijzigingshistorie

VERSIENR	DATUM	REVIEWER	ROL
0.7	23-10-2020	Marc de Goeij	Solution Architect
0.7	05-11-2020	Marco de Haan	Solution Architect
0.8	11-11-2020	Edwin Castelein	Enterprise Architect
0.9	20-11-2020	Edwin Castelein	Enterprise Architect
0.9	20-11-2020	Wesley Cornelissen	CISO
0.9	20-11-2020	Jan Ovink	Inkoper

Tabel 2: reviews

VERSIENR	DATUM	DISTRIBUTIELIJST
0.9	12-11-2020	Michel Bekkers, Edwin Castelein, Wesley Cornelissen, Patrick van der Deijl, Marc de Goeij, Barbara Looten, Eelco van Norren, Jan Ovink
1.0	20-11-2020	Gereed voor publicatie op Tenderned

Tabel 3: distributielijst

INHOUDSOPGAVE

1 INLEIDING 5
1.1 Doel van de Project Start Architectuur 5

2 GEHANTEERDE BEGRIPPEN 6

3 DOEL EN SCOPE PROJECT 9
3.1 Achtergrond 9
3.2 Probleemstelling 9
3.3 Doelstelling 10
3.4 Resultaat 11
3.5 Afbakening 12

4 KADERS EN RICHTLIJNEN 13
4.1 Architectuurprincipes 14
4.2 Standaarden 16
4.3 Bedrijfskaders 18
4.3.1 Bedrijfsfunctiemodel organisatie laag 19
4.3.2 Bedrijfsprocessen en bedrijfsobjecten 20
4.3.3 Bedrijfsrollen 20
4.4 Informatiekaders 22
4.5 Informatiesysteemkaders 24
4.6 Afhankelijkheden andere trajecten 26

5 HUIDIGE ARCHITECTUUR (IST) 27
5.1 Huidig rollenmodel 28
5.2 Aanvraag HANaccount rol Student 29
5.3 Aanvraag HANaccount rol Medewerker 30
5.4 Proces aanvragen abonnement 30
5.5 Matrix rol en abonnementsamenstelling 31

6 TOEKOMSTIGE ARCHITECTUUR (SOLL) 32

7 VERSCHILLENANALYSE (IST/SOLL) 33

8 ROADMAP 34

9 BIJLAGEN 35
9.1 Uitwerking Relatie Projecten en Initiatieven 35

1 INLEIDING

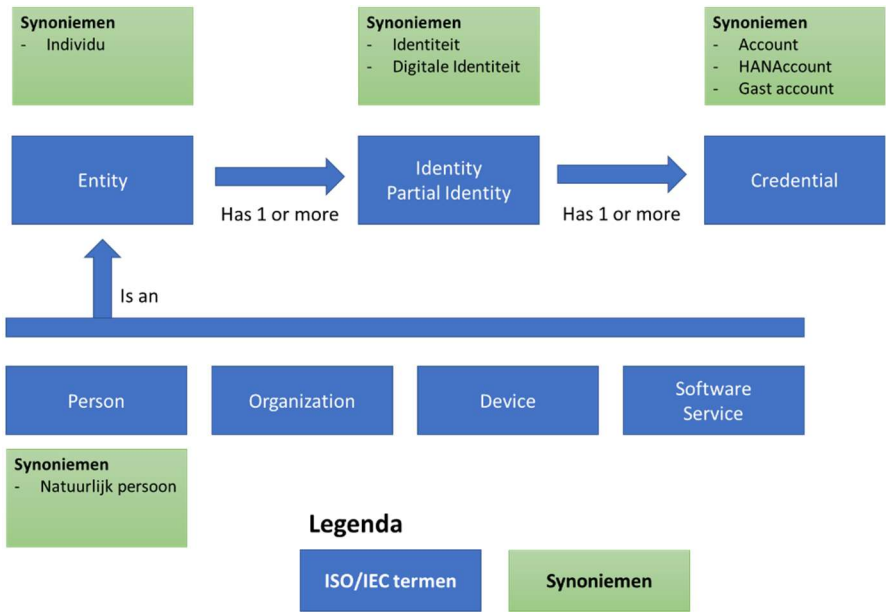
Onderdeel van het Informatiebeleid 2016-2020 is de ambitie om projectstartarchitecturen (PSA) te integreren bij de projectvoorbereiding van informatieprojecten. Samen met het project initiatief document (PID) vormen deze documenten een belangrijke basis voor het projectplan. Het PID vat de opdracht samen, de PSA het ontwerp.
Deze versie van het PSA is onderdeel van de marktconsultatie voor IAM. Het PSA zal aan de hand van input van marktpartijen - die meedoen aan de marktconsultatie - worden aangevuld en waar nodig aangepast.

1.1 Doel van de Project Start Architectuur

De PSA gebruiken we als instrument om te waarborgen dat de HAN nieuwe ontwikkelingen en veranderingen in samenhang realiseert, passend binnen de toekomstig gewenste informatievoorziening en passend binnen kaders en richtlijnen. Door het maken van een globaal ontwerp maken we van een project de ontwerpkeuzes inzichtelijk. Beslissingen hierover geven richting bij het bepalen van de projectscope en planning.

2 GEHANTEERDE BEGRIPPEN

In de projectdocumenten worden verschillende termen gebruikt voor dezelfde begrippen.
Om hier eenduidigheid in te krijgen, worden in Figuur 1 de gehanteerde begrippen en bijbehorende synoniemen uitgelegd aan de hand van de ISO standaard ISO/IEC 24760-1:2019 voor Identity Management (blauwe kaders) en de door de HAN gehanteerde synoniemen (groene kaders).



Figuur 1: Begrip, definitie en synoniem volgens ISO standaard

Bij de termen “Individu” en “Natuurlijk persoon” (of equivalenten daarvan) wordt in de context van IAM feitelijk het begrip **Entity** uit de ISO standaard bedoeld.
Bij de termen “Identiteit” en “Digitale Identiteit” (of equivalenten daarvan) wordt in de context van IAM feitelijk het begrip **Identity** uit de ISO standaard bedoeld.
Bij de termen “Account”, “HANaccount” en “gast account” (of equivalenten daarvan) wordt in de context van IAM feitelijk het begrip **Credential** uit de ISO standaard bedoeld.

De definitie van de drie belangrijkste ISO termen[1] zijn hierna verder uitgelegd:

[1] https://www.iso.org/obp/ui/#iso:std:iso-iec:24760:-1:ed-2:v1:en

3.1.1 Entity
item relevant for the purpose of operation of a domain that has recognizably distinct existence
Note 1 to entry: An entity can have a physical or a logical embodiment.
EXAMPLE:
A person, an organization, a device, a group of such items, a human subscriber to a telecom service, a SIM card, a passport, a network interface card, a software application, a service or a website.

3.1.2 Identity / partial identity
set of attributes related to an entity
Note 1 to entry: An entity can have more than one identity.
Note 2 to entry: Several entities can have the same identity.
Note 3 to entry: ITU-T X1252[13] specifies the distinguishing use of an *identity*. In this document, the term *identifier* implies this aspect.

3.3.5 credential
representation of an identity (3.1.2) for use in authentication (3.3.1)
Note 1 to entry: As described in 5.4, customary embodiments of a credential are very diverse. To accommodate this wide range, the definition adopted in this document is very generic.
Note 2 to entry: A credential is typically made to facilitate *data* authentication of the identity information pertaining to the identity it represents. Data authentication is typically used in authorization.
Note 3 to entry: The identity information represented by a credential can, for example, be printed on human-readable media, or stored within a physical token. Typically, such information can be presented in a manner designed to reinforce its perceived validity.
Note 4 to entry: A credential can be a username, username with a password, a PIN, a smartcard, a token, a fingerprint, a passport, etc.

De ISO standaard onderkent voor een individu meerdere identiteiten.
Ter illustratie gebeurt dit binnen de context van de HAN wanneer een individu zowel binnen de studentenadministratie als binnen de HR-administratie is opgevoerd omdat dit individu zowel werkt als studeert bij de HAN. Dit individu heeft in dit voorbeeld dan twee digitale identiteiten.

De ISO standaard onderkent het toewijzen van meerdere accounts aan een digitale identiteit.
Ter illustratie gebeurt dit binnen de context van de HAN wanneer een medewerker (identiteit) een HANaccount heeft voor de publiek toegankelijke informatiesystemen en een beheeraccount voor servers of het functioneel beheer van een toegangssysteem. Of binnen de context van de HAN aan één individu meerdere HANaccounts of een combinatie van HANaccount en gast account wordt toegekend, is op dit moment nog niet bepaald. In de marktconsultatie komt wellicht meer duidelijkheid over de te volgen lijn hierin.

De ISO/IEC 24760-1:2019 standaard onderkent het begrip rol niet. Daarvoor is een andere standaard, waar deze ISO standaard naar verwijst: ANSI INCITS 359-2004. Volgens deze standaard is het begrip **rol** te omschrijven als:

> A role is a job function within the context of an organization with some associated semantics regarding the authority and responsibility conferred on the user assigned to the role.

Deze standaard stamt uit 2004, waarmee de vraag rijst of de hierboven getoonde definitie nog volledig van toepassing is, of deels maar met toelichting.

De HAN maakt gebruik van de Hay-methode voor functiewaardering en hoewel die methode vanuit HR-perspectief een goede standaard is, blijkt dat er meer variaties gewenst zijn voor een Hay-profiel “Beheerder ICT” en tot welk informatiesysteem een persoon toegang toe heeft. De Enterprise Architectuur van de HAN kent het begrip *bedrijfsrol*. Dat is ook een rol, maar vanuit het perspectief van de Enterprise Architectuur. Hierin komen bedrijfsrollen voor die vergelijkbaar zijn qua naamgeving met een Hay-profiel, waarbij de duiding wel overeenkomt met een Hay-profiel, maar ook hier niet tot eenzelfde set aan toegangsrechten hoeft te leiden bij informatiesystemen.

Een *rol* zoals dat vaak bedoeld wordt in IAM context laat zich het best omschrijven als:

> Een rol beschrijft een samenhangend geheel van activiteiten die door een natuurlijke- of rechtspersoon vervuld kunnen worden. Een (IAM) rol beschrijft de reden waarom een gebruiker toegang krijgt tot bepaalde informatie. Voorbeelden van (IAM) rollen zijn: student, medewerker, stagebegeleider.

Ter illustratie is binnen de context van de HAN een aantal sets van toegangsrechten beschreven voor de verschillende (IAM) rollen die de HAN gebruikt.

3 DOEL EN SCOPE PROJECT

In gesprek met de opdrachtgever, projectleider en de solution architecten is het doel en de scope van het project bepaald. In de aanvang van het project is dit globaal, ruw. Tijdens de uitvoering zal dit verder verfijnd worden waar nodig door o.a. het ophalen van (functionele) requirements uit andere domeinen en projecten. Deze verfijning vindt grotendeels vraag gestuurd plaats.

3.1 Achtergrond

De HAN maakt sinds 2007 gebruik van het huidige Identity Management systeem (IDM) dat door de HAN zelf ontwikkeld is. In de loop der jaren is het systeem uitgebreid met toevoeging van Single Sign On (SSO) en een federatieve koppeling (SURFconext). De basis van het huidige IDM zit in verouderde componenten zoals IMAO, dat vervangen wordt door HAN Integratie Laag (HIL) en diverse provisioningscripts en web portals die verschillende databases en directory services aan elkaar koppelen. Het huidige IDM is de basis van het HANaccount dat iedere deelnemer, medewerker of relatie toegang geeft tot al de informatiesystemen van de HAN, met een logincode en een wachtwoord.

3.2 Probleemstelling

De ambities van de HAN zijn vastgelegd in de HAN doelen en vertaald naar leidende architectuurprincipes. De huidige IDM/IAM omgeving is niet toereikend om deze ambities waar te maken.

- **Onze student staat Centraal**: Om gepersonaliseerd informatie te kunnen verstrekken aan de student die past bij de fase van de studentjourney is het evident dat je ook weet welke student je voor je hebt, of het de juiste student is, en welke fase van de journey de student zich bevindt. Het identificeren van een student alleen is niet meer voldoende. Je dient ook zijn andere identiteiten/rollen te kennen.
- **Responsief onderwijs en onderzoek**: De behoefte aan vergaande flexibilisering, passend bij de behoefte van de student in zijn journey, de veranderende beroepspraktijk, in een flexibele omgeving stelt hoge eisen aan het beheer van de identiteiten. Een veranderende rol bijvoorbeeld kan een groot effect hebben op de autorisaties in de systemen. De identiteit van de student blijft uiteraard hetzelfde maar de rol kan veranderen tijdens zijn journey, van student naar medebeoordelaar of medewerker. Elke rol heeft weer andere rechten.
- **Doelgericht en in verbinding.** De behoefte om meer in hybride leeromgevingen samen te werken leidt ertoe dat niet alleen studenten en medewerkers van de HAN samenwerken maar ook partijen buiten de HAN. Dat geeft nieuwe uitdagingen aan ons IDM/IAM. Het gebruik van identiteiten van collega-instellingen. Wat als wij niet de identiteit beheren maar de student dat zelf doet? Identiteiten van het werkveld?

Aansluitend op de ambities van de HAN: de basis van het huidige IDM-systeem is verouderd. Het belangrijkste component IMAO wordt uitgefaseerd door de HAN Integratie Laag (HIL), als onderdeel van het project Herstructurering Informatie Voorziening Landschap (HIVL). De overige geïntegreerde componenten bestaan uit diverse relationele databases, directory services, web portals en verschillende provisioningscripts. Al deze componenten zijn middels maatwerk door de HAN in de loop der jaren gerealiseerd waarvan het gros door een oud-medewerker. De componenten zijn slecht te onderhouden en daarmee een beveiligingsrisico geworden. Nieuwe teams binnen een academie, de centrale staf of services die een nieuw abonnement of nieuwe worfklow in het AHA-proces willen, kunnen niet zonder ontwikkelaars met een ontwikkeltraject doorgevoerd worden. Nieuwe ontwikkelingen in gebruik nemen met federatieve samenwerking en toepassingen van cloud-oplossingen zijn niet mogelijk zonder opnieuw maatwerk uit te voeren. Er is daarnaast sprake van een kennisleegloop onder key-users die het huidige IDM-systeem destijds ontwikkeld en beheerd hebben.

Deze ontwikkelingen roepen vooral een risico op uitval op, hetzij door verouderde techniek, dan wel door een beveiligingsrisico. Hierdoor kunnen studenten, docenten of ondersteuners niet meer inloggen op informatievoorzieningen van de HAN. Dit is een actueel risico, het hacken en gijzelen van gegevens is helaas een realiteit onder onderwijsinstellingen.

3.3 Doelstelling

Het nieuwe IDM/IAM-systeem heeft als doel om de drie leidende principes uit Figuur 3 te faciliteren. Daarnaast is informatiebeveiliging door recente ontwikkelingen in de maatschappij aan de orde van de dag. De HAN wil dit op duurzame wijze uitvoeren; een IDM/IAM-systeem dat de juiste toegang geeft tot de juiste gegevens aan de juiste gebruikers. De extra doelstelling is flexibilisering in gebruik (zowel intern als extern), als flexibilisering op het gebied van wet- en regelgeving: bij veranderingen in de organisatie of regelgeving ondersteunt het IDM/IAM-systeem i.p.v. dat het frustreert. Met oog op het duurzame aspect biedt het nieuwe IDM/IAM-systeem ruimte voor de trend in toename aan federatieve (internationale) samenwerkingen gebaseerd op standaarden. Technische ontwikkelingen versnellen de flexibilisering van het onderwijs, wie wat waar gedaan heeft, nu doet en straks gaat doen wordt meer ondersteunt door disruptieve ontwikkelingen. Integriteit en betrouwbaarheid zijn daarbij belangrijk en stellen voorwaarden aan een flexibel IDM/IAM-systeem. Dit biedt daarmee een nauwkeuriger inzicht in licentiegebruik waarmee bulk gebruik verkleind kan worden door de juiste rollen of attributen aan de juiste licenties toe te kennen.

3.4 Resultaat

De HAN onderscheidt een aantal resultaatgebieden:

Systeem

1. Een systeem dat de HAN ambities nu en in de toekomst kan ondersteunen.
2. Een veilig IDM/IAM-systeem.
3. Een IDM/IAM-systeem dat flexibel is in gebruik en meebeweegt met de omgeving, meer rollen of anders meer gebruik van relevante attributen voor fijnmaziger toegang “Just In Time, Just Enough Access”: ofwel volgens principes: “least privilege” en “separation of duties”.
4. Aansluiting met federatieve samenwerkingsverbanden op basis van standaarden zoals eduID en eIDAS zonder ontwikkelingen als edubadges uit te sluiten.

Identiteitenbeheer

Voor de authenticatie van identiteiten is de vastlegging in bronsystemen cruciaal. Een deel van het project zal gaan over de vaststelling van de informatiebehoefte uit bronsystemen. (actueel, betrouwbaar, compleet) en de vastleggen van de service in een contract.

5. De bron voor studenten is het SIS.
6. De bron voor medewerkers is eHRM
7. De beoogde bron voor relaties is het CRM

Functionele eisen

8. Door rollen en attributen optimaal toe te passen, wordt de interne flexibilisering eenvoudiger, de decentrale beheerslast kan hiermee verlaagd worden door een fijnmaziger toegangscontrole. De externe flexibilisering maakt toegang tot minoren laagdrempeliger, evenals samenwerking met onderzoekers van verschillende instellingen.
9. De wens van Bring Your Own Device (BYOD) zorgt voor een andere benadering van informatiebeveiliging, niet meer gericht op het apparaat maar op de juiste toegang voor de juiste persoon, onafhankelijk van apparaat.
10. Aansluiting bij de huidige trend van licentiemodellen: betalen naar gebruik per aantal. Door rollen en attributen in te zetten voor een optimale inzet van licenties worden deze niet meer onnodig toegekend en kan dit kostenbesparend werken.

Governance

11. Business rule management. Opstellen van business rules voor het gebruik, beheer, eigenaarschap, randvoorwaarden zoals duur van de autorisatie, rollen en groepen van het nieuwe IDM/IAM systeem.
12. Autorisatiemanagement: Wie geeft akkoord op aanvragen? Hoe loopt dat proces?
13. Functioneel beheer.

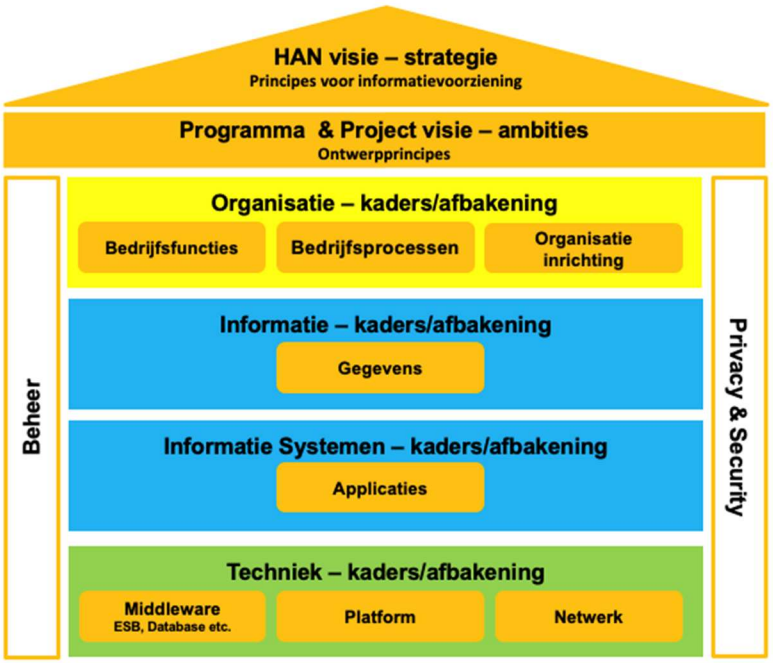
3.5 Afbakening

De afbakening van het project is bij deze versie van de PSA te vroeg in het proces. We willen de opgehaalde informatie uit de marktconsultatie gebruiken om te bepalen wat de invulling zal worden. In een latere fase zal de afbakening daarom vastgesteld worden, omdat de HAN geen uitsluitingen wil maken van concepten of oplossingen die ze niet op de radar heeft.

4 KADERS EN RICHTLIJNEN

Het implementeren van een veranderinitiatief dient te passen binnen de HAN-inrichting. Om dat te concretiseren maken we gebruik van verschillende kaders en richtlijnen. Deze bestaan op verschillende niveaus zoals op bedrijfsfunctie, applicatie of gegevensniveau. Zij helpen bij het kaderen van het project maar leggen ook dwingend beperkingen op. Kaders en richtlijnen bevatten geen wetmatigheden maar passen onder het principe “pas toe of leg uit”. De architectuurkaders staan in de HAN Enterprise Architectuur en zijn afgestemd op de referentiemodellen van de HORA[2] IDM/IAM is een belangrijk thema met het oog op de flexibiliseringsambitie in het hoger onderwijs. Om die reden wordt een landelijke sectorarchitectuur opgesteld, de HOSA[3]. De intentie is dat de HAN zich daaraan zal conformeren.

Binnen de HAN worden de diverse architectuurconcepten en -aspecten toegepast volgens het model in Figuur 2, in de wandelgangen bekend als “het huisje”. IDM/IAM gaat namelijk niet alleen over de aanschaf van een systeem maar de inbedding in het IV-landschap in al haar facetten.

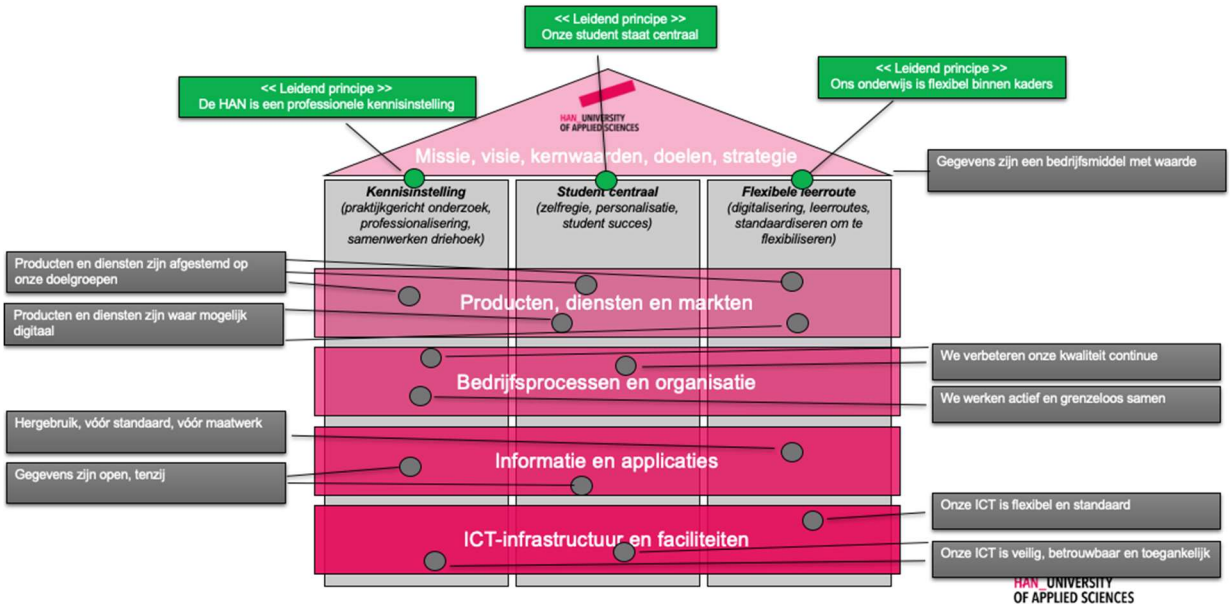


Figuur 2: architectuurkaders en positie binnen de HAN

[2] https://hora.surf.nl/index.php/Hoofdpagina
[3] https://www.surf.nl/cooperatie-surf/versnellingsplan-onderwijsinnovatie-met-ict en https://versnellingsplan.nl

4.1 Architectuurprincipes

De HAN heeft architectuurprincipes vastgesteld en deze uitgewerkt in diverse regels en richtlijnen. In het ontwerp zijn deze richtlijnen gehanteerd. De leidende principes zijn afgeleid van de strategische thema's van de HAN. Principes versterken elkaar als een geheel tot het fundament aan toe (Figuur 3). Deze leidende principes recentelijk vernieuwd en dienen nog door het College van Bestuur van de HAN definitief te worden vastgesteld. Desalniettemin is er bewust voor gekozen om de leidende principes wel toe te passen omdat deze afgeleid zijn uit het Instellingsplan 2016-2022[4]. Daarnaast is de verwachting dat de principes grotendeels ongewijzigd zullen worden vastgesteld. Wanneer het College van Bestuur aanpassing vraagt, wordt deze meegenomen in dit ontwerp.



Figuur 3: Architectuur- en leidende principes van de HAN

De principes die van toepassing zijn en waarom zijn toegelicht in Tabel 4:

[4] https://www.han.nl/over-de-han/missie-en-strategie/instellingsplan/

De HAN kent **drie leidende principes** die richting geven aan het totaal van principes (Tabel 4).

Nr.	Principe	Relevant?	Toelichting
1	**Onze student staat centraal**	Ja	Student krijgt de juiste toegang meer op maat toegesneden, veilig; niet te veel informatie, wel de juiste.
2	**De HAN is een professionele kennisinstelling**	Ja	Leren, werken en onderzoeken in de driehoek worden gefaciliteerd om samen te werken binnen en buiten de HAN.
3	**Ons onderwijs is flexibel binnen kaders**	Ja	Voldoen aan randvoorwaarden voor flexibilisering volgens het Versnellingsplan[5]
4	Gegevens zijn een bedrijfsmiddel met waarde	Ja	Identiteiten met autorisaties zijn het essentieel voor de gehele informatievoorziening.
5	Producten en diensten zijn afgestemd op onze doelgroepen	Ja	Faciliteren i.p.v. frustreren van onlinesamenwerking met de juiste toegang tot de juiste doelgroep.
6	Producten en diensten zijn waar mogelijk digitaal	Ja	IDM/IAM is per definitie digitaal en de eerste toegang tot digitale informatievoorzieningen. Waar nodig wordt gezocht naar verbinding met de fysieke wereld
7	We verbeteren onze kwaliteit continue	Ja	Een veilig IDM/IAM-systeem is een eerste vereiste, gegevens alleen ontsluiten aan de juiste doelgroep en inzicht hebben daarin te allen tijde om te sturen daarop.
8	We werken actief en grenzeloos samen	Ja	IDM/IAM is de fundering waarmee actief en grenzeloos (in meerdere betekenissen) samengewerkt kan worden, federatief en in de driehoek.
9	Hergebruik, vóór standaard, vóór maatwerk	Ja	Het huidige IDM is verouderd, hergebruik daarvan, of componenten is ongewenst, evenals nieuw maatwerk. Er is geen systeem beschikbaar dat hergebruikt kan worden.
10	Gegevens zijn open, tenzij	Ja	Om gegevens open te kunnen stellen aan de juiste doelgroep met de juiste set aan data maakt het IDM/IAM-systeem dit mogelijk.
11	Onze ICT is flexibel en standaard	Ja	Informatievoorzieningen kunnen eenvoudig en snel van de juiste autorisatie voorzien worden middels administratieve handelingen i.p.v. maatwerk.
12	Onze ICT is veilig, betrouwbaar en toegankelijk	Ja	IAM-systeem faciliteert veilige toegang, op betrouwbare wijze door “just enough access” grof- en fijnmazig mogelijk te maken voor de juiste doelgroep.

Tabel 4: architectuurprincipes van de HAN

[5] Zie ook: https://www.surf.nl/cooperatie-surf/versnellingsplan-onderwijsinnovatie-met-ict

4.2 Standaarden

De toepassing van standaarden bevorderd gegevensuitwisseling en samenwerking intern en extern. Gegevens kunnen hierdoor veilig, betrouwbaar en eenvoudig gedeeld worden. Dit komt de flexibiliteit van het onderwijs ten goede. Door standaarden in te zetten is er doorgaans geen afhankelijkheid van één leverancier. De volgende standaarden voor gegevensuitwisseling (**Fout! Verwijzingsbron niet gevonden.**) en beveiliging (Tabel 6) zijn relevant[6] voor dit veranderinitiatief:

STANDAARD	TOELICHTING
DAI, ORCID	De Digital Author Identifier is een uniek landelijk nummer voor elke onderzoeker werkzaam bij een Nederlandse instelling. ORCID is een internationaal initiatief maar behoeft stimulatie. **Relevant bij onderzoekssamenwerking, identificeert onderzoeker.**
E-portfolio NL	Competenties van een individu kunnen meegenomen worden naar verschillende organisaties, relevant voor digitale leeromgeving. **Relevant voor eduID, edubadges, identificeert deelnemer**
OData	Open protocol voor het ontwikkelen van, en integratie met REST API's. **Relevant voor een flexibele en standaard wijze van koppelen, ontsluiten, provisioning.**
SCIM	System for Cross-domain Identity Management. Automatiseren van provisioning, inclusief attributen, schema's en groepslidmaatschap. **Relevant voor lifecycle management van identiteiten en autorisaties voor personen.**
SETU	Nederlandse implementatie voor internationale HR-XML standaard, ontwikkeld door grote uitzendorganisaties. Biedt uniformering van uitwisseling gegevens over inhuur van tijdelijk personeel, leidt tot vereenvoudiging inhuurproces. **Relevant bij provisioning middels SCIM, identificeert tijdelijk personeel.**
Semantisch model e-factureren	Standaard voor elektronisch factureren. Heeft relatie met SETU. **Mogelijk relevant bij digitale HANcard en open betaalsysteem, identificeert verrekening per individu.**
VOOT	Koppeling van een externe group provider met SURFconext en de uitwisseling van groepsinformatie. **Relevant voor een flexibele en persoonlijke leer- en werkomgeving.**

Tabel 5: Relevante standaarden Gegevensuitwisseling

[6] https://standaarden.surf.nl/index.php?title=Relevante_standaarden

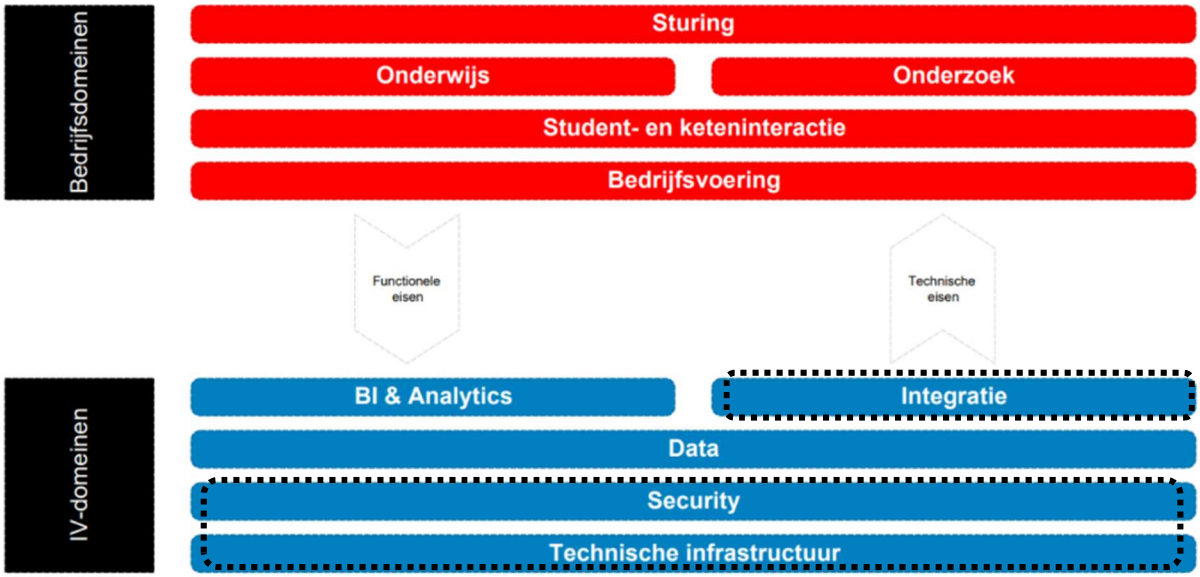
STANDAARD	TOELICHTING
INCITS 359	Standaard voor Role Based Access Control. **Relevant voor een flexibele en persoonlijke leer- en werkomgeving.**
IRMA	Privacy-vriendelijke methode voor attribuut-gebaseerd identity management. **Relevant voor toepassen wet- en regelgeving (AVG).**
NEN-ISO/IEC 27001	Uniformerend voor informatiebeveiligingsbeleid, voor duidelijkheid in relatie tussen leveranciers en opdrachtgever. **Relevant voor toepassen wet- en regelgeving.**
NEN-ISO/IEC 27002	Nadere specificatie van de NEN-ISO/IEC 27001. **Relevant voor toepassen wet- en regelgeving.**
OAuth, UMA	Maakt het mogelijk de gebruiker een (mobiele) applicatie op een veilige manier namens hemzelf toegang te geven tot een datastore. **Relevant voor een flexibele en persoonlijke leer- en werkomgeving, en Leven Lang Leren (UMA).**
OpenID(connect)	Aanvulling op OAuth, gericht op mobiele (web) applicaties. **Relevant voor een flexibele en persoonlijke leer- en werkomgeving.**
SAML	Veelgebruikte standaard op het gebied van Identity Management, basis van SURFconext. **Relevant voor identificatie van een persoon met rechten en attributen.**
XACML, NGAC	Fijnmazig Attribute Based Access Control Policy (ABAC) op basis van attributen. **Relevant voor flexibele autorisatie van een persoon, ondersteunend bij audits.**

Tabel 6: Relevante standaarden Beveiliging

De daadwerkelijke relevantie van de standaarden in **Fout! Verwijzingsbron niet gevonden.** en Tabel 6 zal duidelijker worden naarmate er informatie uit de marktconsultatie en afstemming met stakeholders is geweest. Met name Attribute Based Access Control (ABAC) is een driver om te bepalen in hoeverre deze standaarden van toepassing zijn omdat ABAC nu nog niet breed toegepast worden binnen de HAN, maar dit wel aan de ambities kan bijdragen.

4.3 Bedrijfskaders

De HAN Enterprise Architectuur onderkent een aantal domeinen met een grove indeling op *Bedrijfsdomeinen* en *IV-domeinen.* Van deze domeinen is er een brede en een smalle scope relevant bij dit veranderinitiatief. De smalle scope omvat de domeinen die direct betrokken zijn bij de implementatie, deze zijn randvoorwaardelijk om het project uit te kunnen voeren. Deze smalle scope is zwart omcirkeld in Figuur 4. De brede scope omvat alle overige domeinen die afnemer zijn van IAM. Deze overige domeinen kunnen ook leverancier zijn. De functionele behoefte voor klant en leverancier dient opgehaald te worden in de uitvoering van dit project.

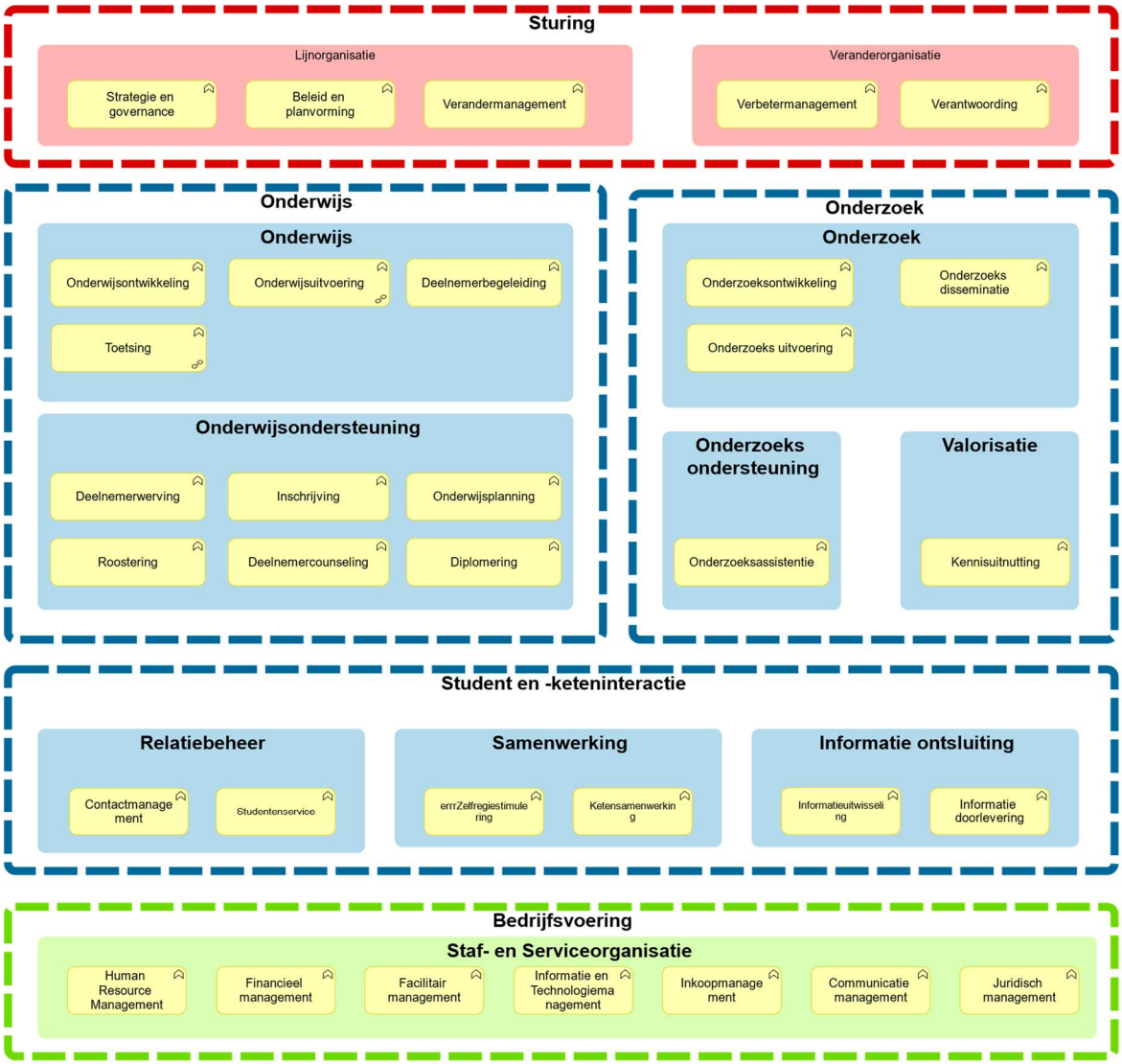


Figuur 4: domeinen binnen architectuur van de HAN

Uit de functionele behoeften van andere domeinen kunnen requirements leiden voor het IAM-project. Andersom is ook mogelijk: het project kan eisen stellen aan bijvoorbeeld het bedrijfsvoeringdomein. Bijvoorbeeld: zonder eenduidige vastlegging van gegevens in het HR-bronsysteem is het IAM-systeem niet duurzaam of betrouwbaar. Dit vereist wellicht procesafspraken rondom de registratie van alle medewerkers; zowel intern als extern en in welk bronsysteem?

4.3.1 Bedrijfsfunctiemodel organisatie laag

De bedrijfsfuncties per domein, die geraakt worden door dit veranderinitiatief, zijn in deze fase van het project lastig vast te stellen; in feite zijn alle bedrijfsdomeinen relevant (Figuur 5). Welke bedrijfs(sub)functies betrokken zijn, en in welke mate met welk proces, kan bepaald worden na het ophalen van functionele behoefte uit de business en wanneer duidelijk is welke eisen IAM stelt aan de bedrijfsdomeinen.



Figuur 5: Bedrijfsfunctiemodel Bedrijfsdomeinen in de HAN Enterprise Architectuur

4.3.2 Bedrijfsprocessen en bedrijfsobjecten

Bedrijfsprocessen en -objecten op IV-domein Security zijn nog niet gedefinieerd binnen onze Enterprise Architectuur. Zoals in paragraaf 4.3 en 4.3.1 aangegeven moet eerst de functionele behoefte opgehaald worden uit de bedrijfsdomeinen. Wanneer dat gedaan is en dat nodig is, worden deze gedefinieerd en hier opgenomen. Een eerste stap zou zijn het identificeren van processen waar de identiteit een extra rol speelt, zoals deelname aan toetsen, toegang tot gebouwen of stagebegeleiding.

4.3.3 Bedrijfsrollen

In de context van IDM/IAM is het gebruikelijk dat Access Management (toegangsrechten) wordt toegepast middels groepen. Toegangsrechten zijn gebaseerd op de rol van de gebruiker. Rollen worden geïmplementeerd middels groepen. De HAN heeft in 2007 een set toegangsrechten vastgesteld voor verschillende organisatie brede informatiesystemen. Deze toegangsrechten zijn bij de HAN abonnementen genoemd, ze kennen een start- en einddatum van geldigheid. De standaard geldigheidsduur is 1 jaar. Een groepering van abonnementen is voor de meest voorkomende doelgroepen van de HAN gelijk; deelnemer en medewerker. Dit maakt dat deelnemers en medewerkers hun eigen vaste set aan abonnementen krijgt.

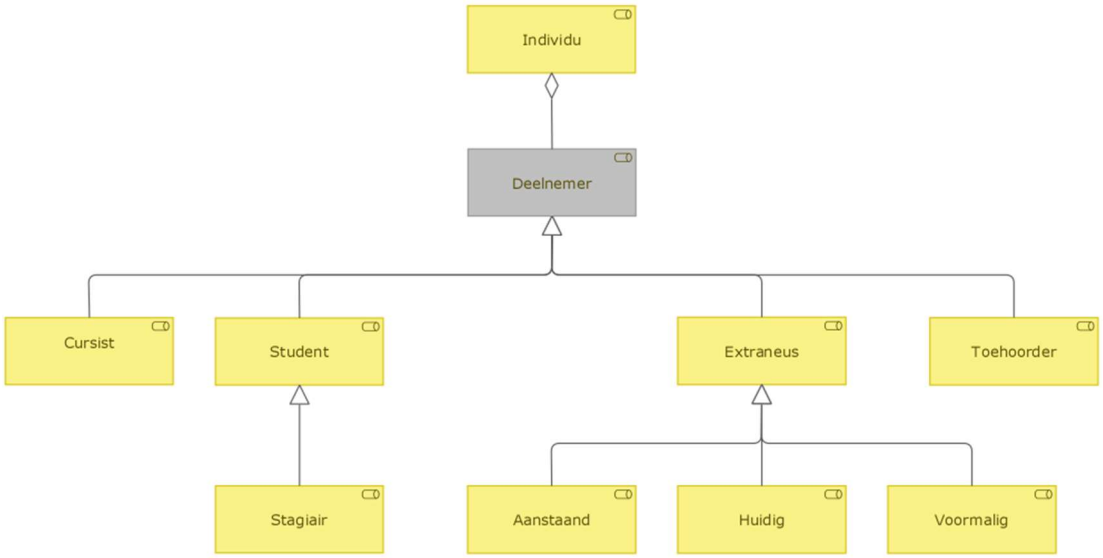
Dit concept van “een vaste set aan abonnementen definieert een specifieke rol” heeft er toe geleid dat de HAN hoofdzakelijk 5 rollen heeft vastgesteld voor de hele organisatie en specifieke abonnementen decentraal toepast bij applicaties of functies die een kleinere doelgroep bedienen (zie ook Figuur 14 in paragraaf 5.1: Huidig rollenmodel).

Om bij te kunnen dragen aan de doelen en het resultaat van dit IAM-project is meer onderscheid nodig tussen rollen en de verschillende journeys. Dit kan betekenen dat er meer abonnementen of meer rollen vastgesteld moeten worden. Maar het kan ook betekenen dat Role Based Access Control alleen niet volstaat, een opkomende manier om dit onderscheid te kunnen maken, is (in combinatie) met Attribute Based Access Control. Bijvoorbeeld in combinatie met dynamische groepen op basis van attributen. De rol geeft grofmazig aan wat de binding van een persoon met de HAN is; studeren, werken of begeleiden. Een attribuut kan aangeven waar een persoon dat doet (opleiding, afdeling) of in welke functie (docent, ondersteuner, leidinggevende). De marktconsultatie zal uitwijzen of de fijnmazigheid als rol of als (tijdelijk) attribuut gebruikt kan worden binnen de lifecycle van een identiteit. Attributen als “Is Manager” of “Is Medewerker Financien” kunnen ondersteunend werken naast de rol “Medewerker” in applicaties en (de)centrale beheerslast en de kans op fouten daarbij verlagen. Attributen als “Is Student” of “Is Onderzoeker” ondersteunen federatieve samenwerking door voor elke Service Provider de juiste set aan attributen (en niet meer dan nodig) uit te wisselen. Dit soort toepassingen maakt een persoonlijke benadering sterker bij gebruikers die bijvoorbeeld met *feedforward* en *feedback* ondersteund kunnen worden in hun digitale ervaring bij de HAN: “Om toegang te krijgen tot deze

informatiebron voor studenten, *klik hier.*". Attributen kunnen ook bijdragen in applicaties die proces georiënteerd werken i.p.v. taak georiënteerd, afhankelijk van attributen krijgt de gebruiker in een Studenten Informatie Systeem (SIS) de proces flow gepresenteerd in de context van de attributen.

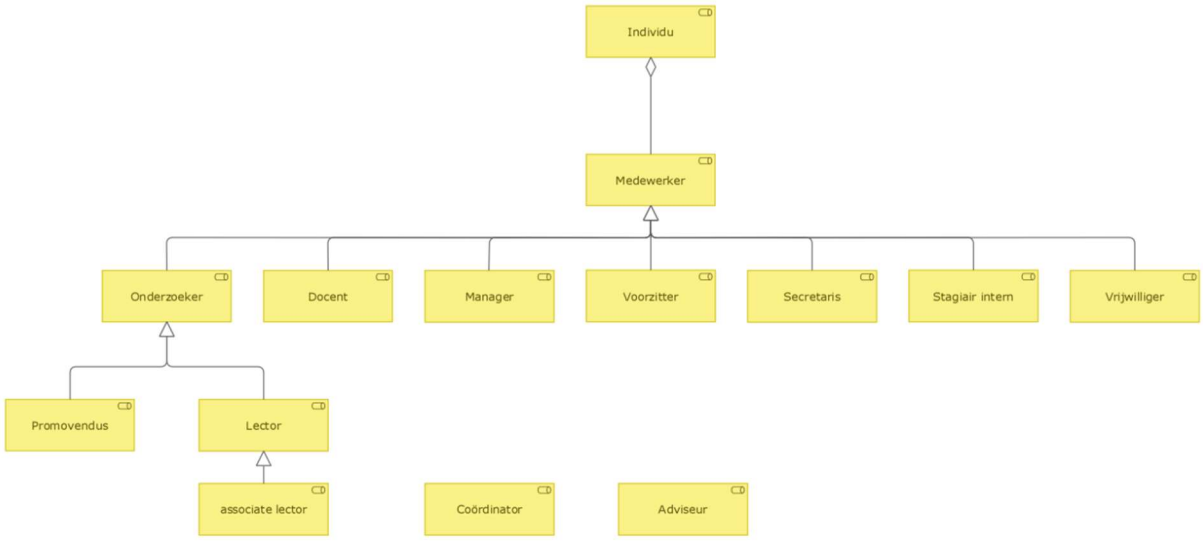
In Figuur 6, Figuur 7 en Figuur 8 zijn een aantal voorbeelden getoond van een rollenmodel dat met de bedrijfsdomeinen afgestemd moet worden aan de hand van opgehaalde functionaliteit.

Voorbeeld rollenmodel Deelnemer



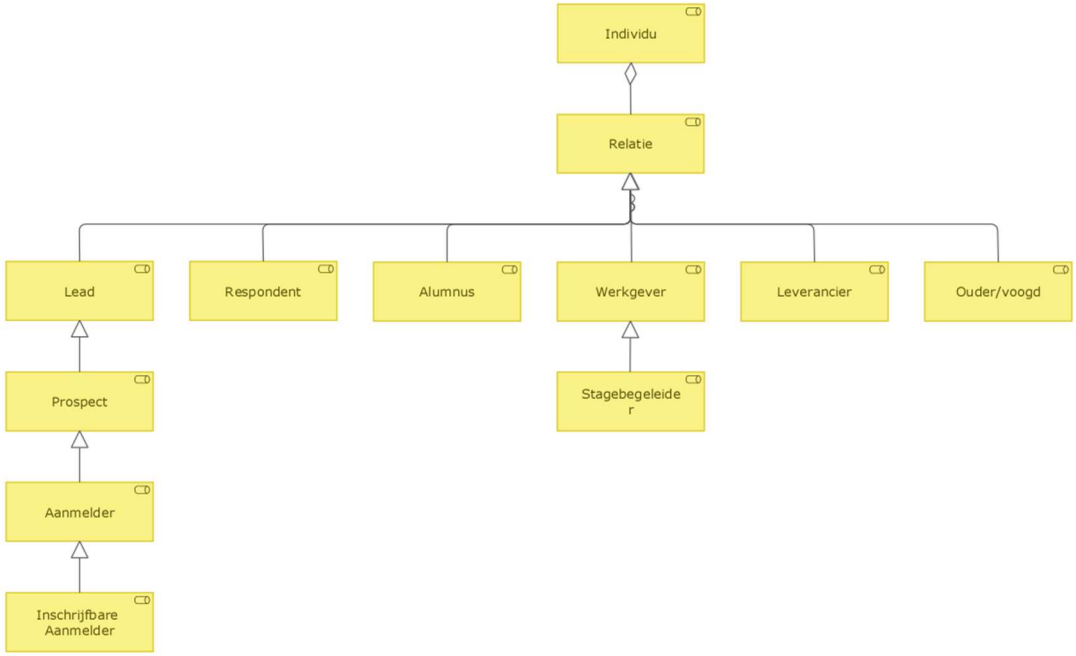
Figuur 6: Voorbeeld rollenmodel Deelnemer

Voorbeeld rollenmodel Medewerker



Figuur 7: Voorbeeld rollenmodel Medewerker

Voorbeeld rollenmodel Relatie



Figuur 8: Voorbeeld rollenmodel Relatie

4.4 Informatiekaders

De HAN heeft als onderwijsinstelling te maken met diverse bedrijfs(sub)functies, -processen en -objecten waar gegevens uitgewisseld worden. Veel componenten binnen een architectuur kennen een interface welke gebaseerd zijn op datadefinities. Een goede kwaliteit van de kerngegevens in processen en systemen bevorderd een eenduidige ketenintegratie en dit maakt ook service oriëntatie mogelijk. Hiertoe heeft de HAN *generieke begrippen* beschreven. Deze *generieke begrippen* zijn de start geweest voor de ontwikkeling van het *Canoniek Datamodel*. Daarbij is een onderscheid gemaakt tussen *specifieke data* en *canonieke data*. Canonieke data is de data die belangrijk geacht wordt door meerdere stakeholders in de organisatie. In het Engels wordt ook de term *Master Data* gebruikt. Vanuit data-architectuur wordt de volgende definitie gebruikt: *een canoniek datamodel is een beschrijving van herbruikbare, generieke en gestandaardiseerde (data-) objecten binnen een interface. Een interface wordt hierbij beschouwd als een punt van interactie tussen architectuurconcepten.*

Het Canonieke Datamodel van de HAN is in ontwikkeling. Het Canonieke Datamodel heeft een samenhang met de bedrijfsobjecten zoals toegelicht in paragraaf 4.3.2 hierboven. Wanneer de bedrijfsprocessen en -objecten gedefinieerd zijn binnen onze Enterprise Architectuur is de samenhang met de relevante canonieke entiteiten te duiden.

De HAN heeft generieke begrippen[7] vastgesteld volgens het bedrijfsfunctiemodel en per domein weergegeven. Deze generieke begrippen worden ook wel aangeduid met de term *Master Data Objecten*. De volgende generieke begrippen zijn relevant voor dit veranderinitiatief (Tabel 7 en Tabel 8):

	BEGRIP	GENERIEK	FINANCIEEL	HR	ORGANISATIE	ONDERZOEK	FACILITAIR	ONDERWIJS	RELATIEBEHEER
1.	Aanmelding								x
2.	Alumnus								x
3.	Autorisatie						x		
4.	Cursist	x							
5.	Deelnemer	x				x		x	x
6.	Externe medewerker	x	x	x		x		x	x
7.	Externe organisatie	x	x	x	x	x	x	x	x
8.	Functie	x	x	x	x	x		x	
9.	Groep	x	x	x	x	x	x	x	
10.	Herinschrijving							x	
11.	Individu	x	x	x	x	x	x	x	x
12.	Inschrijfvoorwaarde							x	
13.	Inschrijving							x	
14.	Intekening							x	
15.	Interne medewerker	x	x	x		x		x	
16.	Intrekking verzoek tot inschrijving							x	
17.	Lead								x
18.	Leidinggevende			x					
19.	Locatie						x		
20.	Medewerker	x	x	x	x	x	x	x	x
21.	Opleiding	x			x	x		x	x
22.	Organisatieonderdeel	x	x	x	x	x	x	x	
23.	Organisatieonderdeeltaak				x				
24.	Promovendus					x			
25.	Relatie								x
26.	Rol		x						
27.	Ruimte	x				x	x	x	

7 https://hannl.sharepoint.com/teams/EnterpriseArchitectuur/Gedeelde%20documenten/Informatie/CDM/hydra-cdm-v1.0.pdf

28.	Student	x	x		x	x		x	x
29.	Uitschrijving							x	
30.	Verzoek tot herinschrijving							x	
31.	Verzoek tot inschrijving							x	
32.	Verzoek tot uitschrijving							x	

Tabel 7: Generieke begrippen per domein in smalle scope als bouwsteen voor IAM

De generieke begrippen in Tabel 7 vallen in de smalle scope waarmee identiteiten en attributen in hun *identity life cycle* geïdentificeerd kunnen worden.

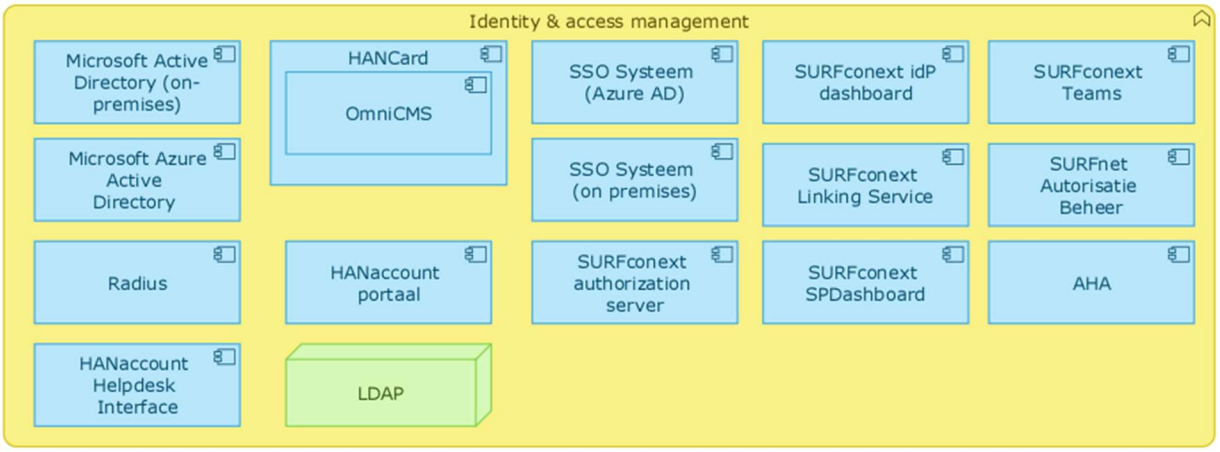
	BEGRIP	GENERIEK	FINANCIEEL	HR	ORGANISATIE	ONDERZOEK	FACILITAIR	ONDERWIJS	RELATIEBEHEER
1.	Bewaartermijn						x		
2.	Dienst						x		
3.	Formatie			x					
4.	Mandaat						x		
5.	Middel						x		
6.	Minor							x	
7.	Module							x	
8.	Onderwijsactiviteit							x	
9.	Opleidingsvariant							x	x
10.	Toetsuitvoering							x	

Tabel 8: generieke begrippen per domein in brede scope als klant/leverancier van IAM

De generieke begrippen in Tabel 8 vallen in de brede scope als tijdelijke attributen die ondersteunend zijn aan de persoonlijke gebruikerservaring voor de juiste toegang tot de juiste set aan gegevens (in het juiste tijdsvenster).

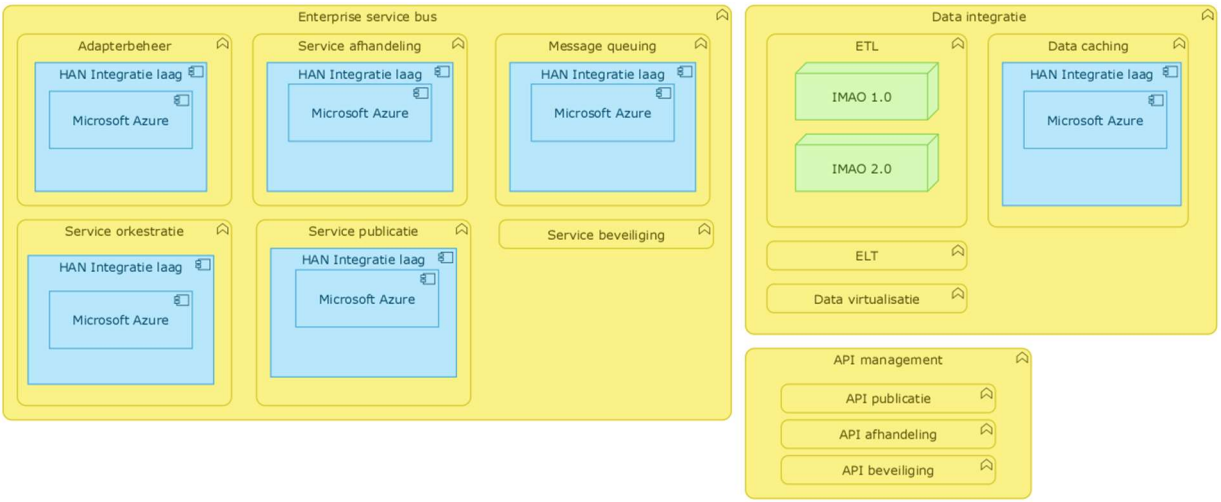
4.5 Informatiesysteemkaders

De aanwezige applicaties per bedrijfssubfunctie in de randvoorwaardelijke IV-domeinen zijn weergegeven in Figuur 9, Figuur 10 en Figuur 11. Deze applicaties geven niet de huidige architectuur van het huidige IDM-systeem weer, maar geven een beeld van de applicaties per bedrijfssubfunctie waar het nieuwe IAM-systeem mogelijk mee zal integreren.



Figuur 9: Applicatiemodel IV domein Security

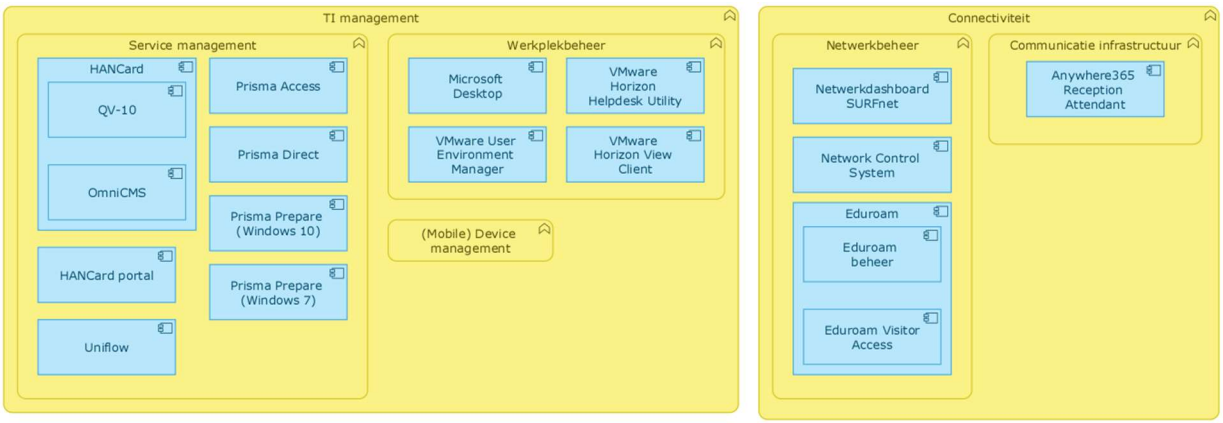
De applicaties in Figuur 9 zijn de applicaties die deels het huidige IDM-systeem realiseren.



Figuur 10: Applicatiemodel IV domein Integratie

Het huidige IDM maakt gebruik van technologiecomponent *IMAO 1.0* en voor sommige delen van een door de HAN zelfgemaakte API[8] (Figuur 10).

[8] https://api.han.nl

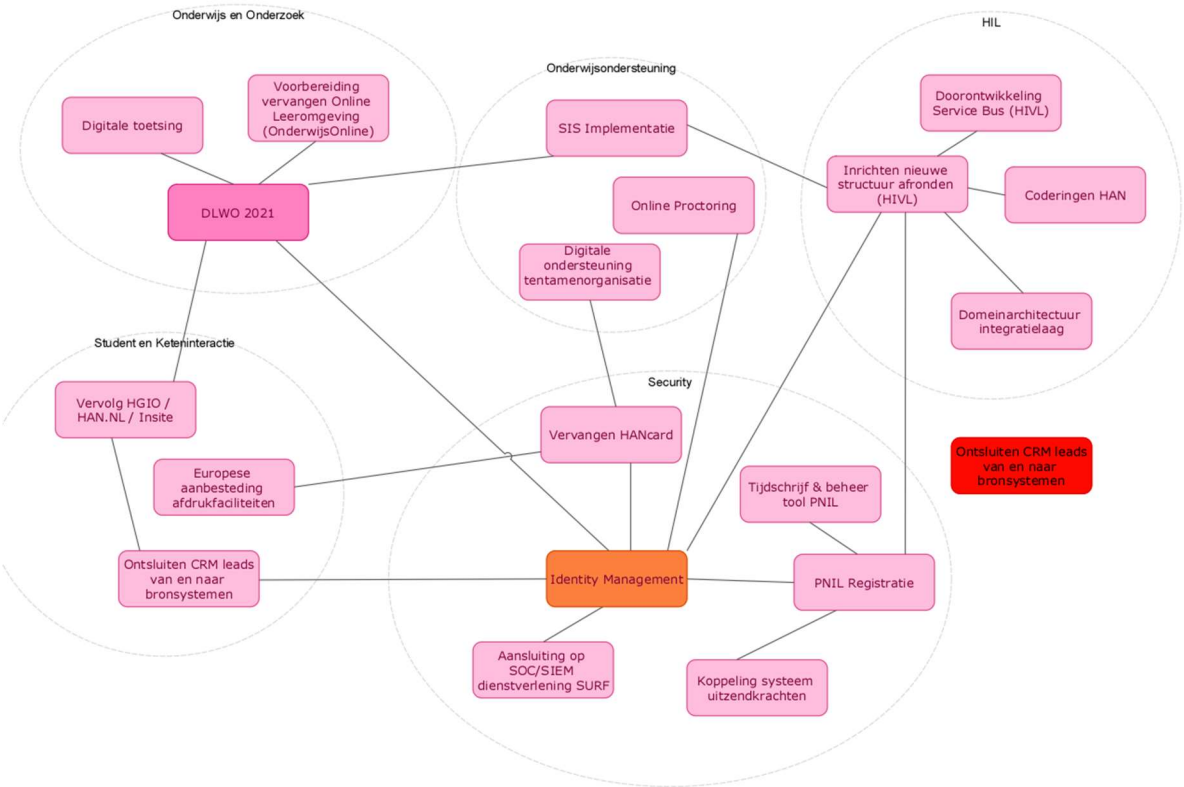


Figuur 11: Applicatiemodel IV domein Technische Infrastructuur

Om gebruik te kunnen maken van VMware Horizon wordt gebruik gemaakt van radius en LDAP (Figuur 9), toegang tot het draadloze netwerk (eduroam) wordt ook middels deze componenten gerealiseerd. Voor follow-me-printing dient de HANcard i.c.m. workflow en een gesloten betaalsysteem (Figuur 11).

4.6 Afhankelijkheden andere trajecten

In de projectportefeuille van de HAN tussen 2021 en 2024 zijn de lopende projecten en initiatieven in kaart gebracht die direct of indirect gerelateerd zijn aan het project IDM/IAM (Figuur 12).



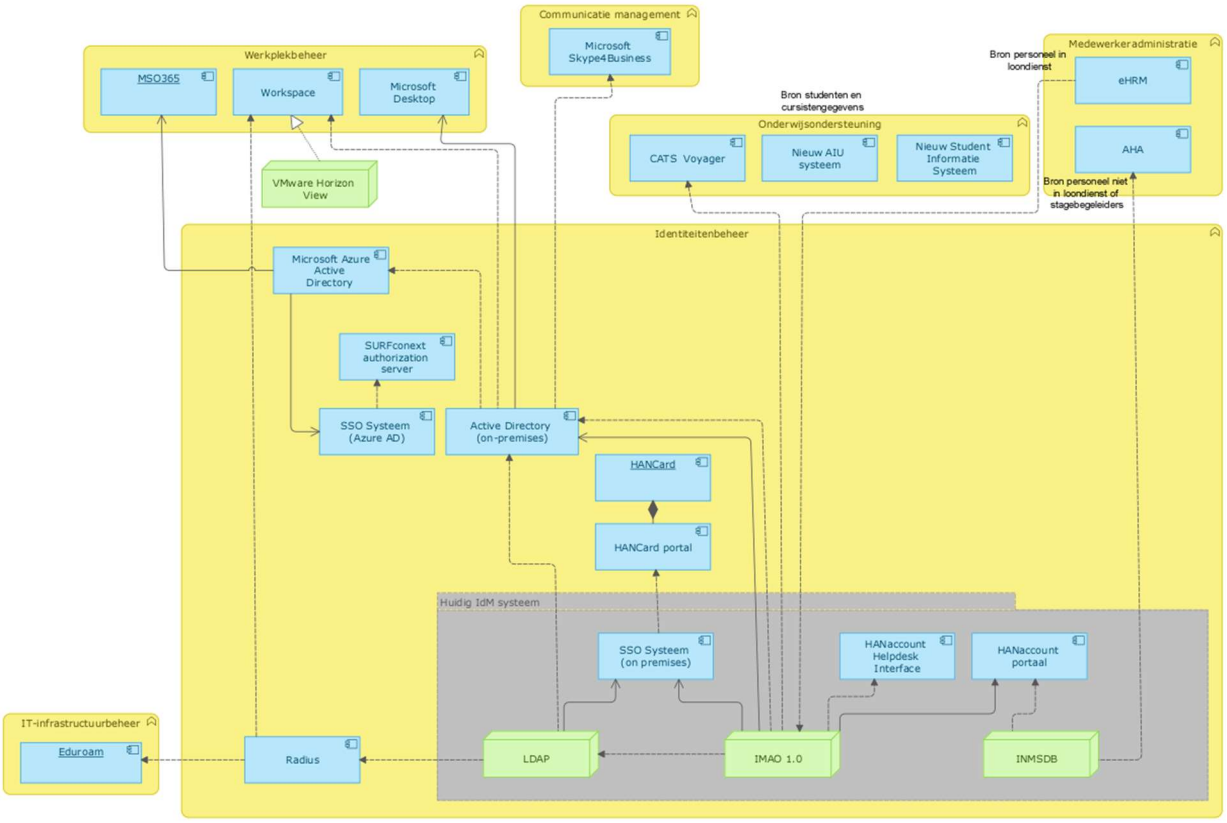
Figuur 12: Samenhang projecten met IDM/IAM

De projecten en de relatie met het IDM/IAM project worden beschreven in bijlage 9.1 van dit document.

5 HUIDIGE ARCHITECTUUR (IST)

De huidige architectuur is verdeeld over 6 bedrijfs(sub)functies en kent 3 bronnen om een identiteit te creëren (Figuur 13**Fout! Verwijzingsbron niet gevonden.**). Deze 3 bronnen zijn:

1. CATS Voyager: bron van in- en uitschrijving van studenten en cursisten.
2. eHRM: bron van personeel in loondienst (PIL oftewel interne medewerker).
3. AHA: bron van personeel niet in loondienst (PNIL oftewel externe medewerker) of externe personen die een relatie met de HAN hebben zoals stagebegeleiders.



Figuur 13: Huidige architectuur (IST)

Het huidige IDM-systeem is grijs omkaderd en verzorgt de creatie van identiteiten middels een selfservice concept. Iedere relatie van de HAN (student, medewerker of anders) maakt zelf een HANaccount aan in het HANaccount portaal. Vervolgens kan deze persoon zelf het HANaccount opwaarderen naar de juiste rol, of een abonnement aanvragen. Elke bron kent een eigen workflow waarmee dat opwaarderen slaagt of niet. Deze workflows zijn gebaseerd op een hiërarchische organisatiestructuur met op elke laag een organisatieonderdeel van de HAN met daarbij één of meerdere gemandateerde personen die geïnformeerd worden als een persoon een rol of abonnement aanvraagt. Normaliter zal voor het gros van de personen het opwaarderen automatisch gebeuren op basis van een aantal kenmerken die de HAN voortijdig aan hen verstrekt heeft.

In het gele kader van de bedrijfssubfunctie *Identiteitenbeheer* zijn de applicatiecomponenten opgenomen die een (aanvullende) autorisatiecontrole uitvoeren. De applicatiecomponenten of bedrijfssubfuncties waarvoor dat gebeurd is in de andere geel gekaderde bedrijfs(sub)functies weergegeven: *Werkplekbeheer, Communicatie Management, Onderwijsondersteuning, Medewerkeradministratie en IT-infrastructuurbeheer*. De applicatiecomponenten in Figuur 13 die in deze andere geel gekaderde bedrijfs(sub)functies zijn weergegeven geven een indicatie weer van de reikwijdte van het huidige applicatielandschap rondom IDM.

In het gele kader van de bedrijfsfunctie *Onderwijsondersteuning* staan twee applicatiecomponenten genoemd waarvan een aanbestedingstraject loopt. Dit zijn “Nieuw AIU systeem” en “Nieuw Student Informatie Systeem”. Deze zullen de functie van “CATS Voyager” binnen een aantal jaar vervangen. De wijze waarop dat zal plaatsvinden is onderdeel van die aanbesteding.

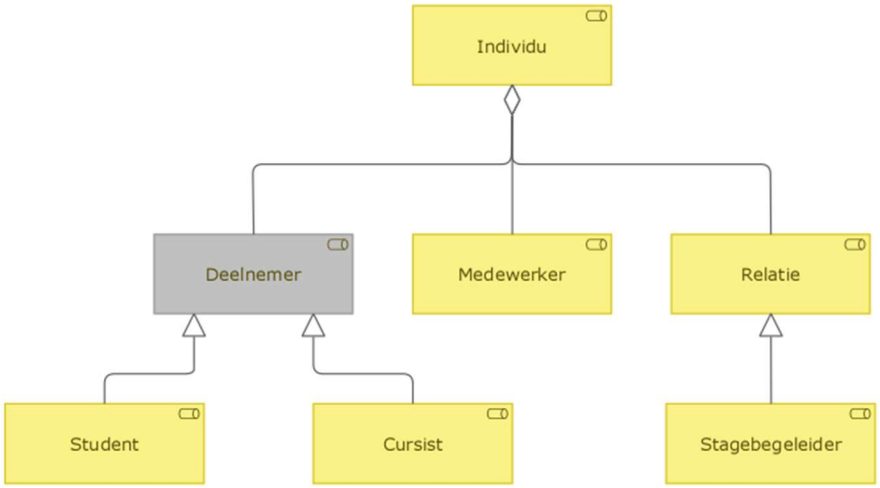
De twee groene nodes *IMAO 1.0* en *INMSDB* zijn relationele databases. De eerste is de centrale data store van de HAN waarbij middels ETL-processen gegevens in- en uitgaan. De tweede wordt gebruikt om applicatiedata en -workflow van “HANaccount portaal” en “AHA” vast te leggen. De centrale data store *IMAO* wordt vervangen door een enterprise service bus (HAN Integratie Laag), het huidige IDM-systeem maakt daar nog geen gebruik van. Het nieuwe IAM-systeem zal dat mogelijk wel gaan doen, afhankelijk van de reacties van de marktpartijen.

5.1 Huidig rollenmodel

De HAN kent vijf verschillende rollen die nu toegepast worden in het huidige IDM-systeem:

1. Student (specialisatie van Deelnemer)
2. Cursist (specialisatie van Deelnemer)
3. Medewerker
4. Relatie
5. Stagebegeleider (specialisatie van Relatie)

Deze vijf rollen zijn geaggregeerd in een Individu (Figuur 14). In dat figuur is Deelnemer grijs weergegeven omdat deze niet als zelfstandige rol gebruikt wordt in het huidige IDM-systeem.

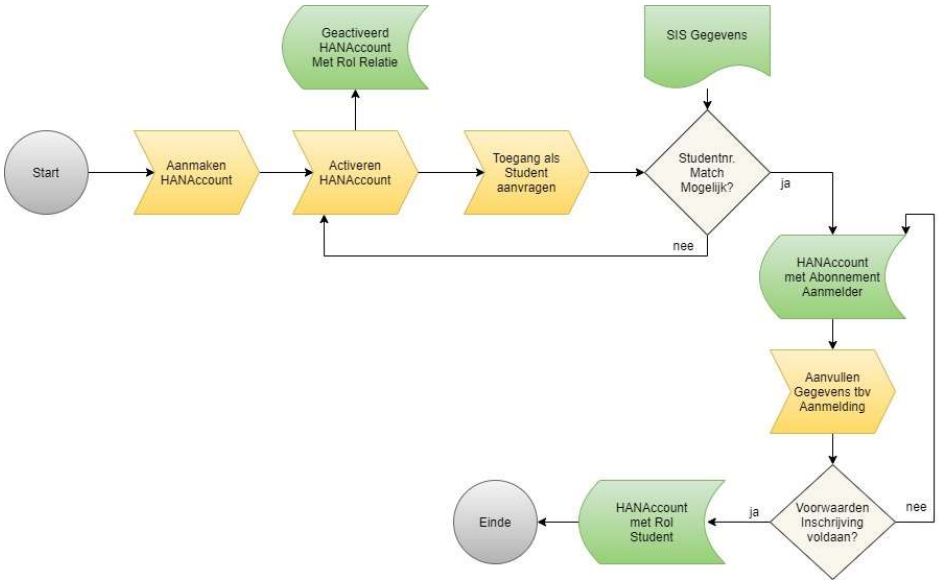


Figuur 14: Rollenmodel HAN grofmazig

Eén individu kan volgens het model meerdere rollen hebben, in het verleden is dat ook het beleid geworden. Echter blijkt dat dit na verloop van tijd voor problemen zorgt in sommige applicaties. De ene applicatie maakt het mogelijk om bij de start een proces flow te kiezen voor een van de actieve rollen en waarborgt daarna gedurende de sessie dat alleen de gekozen rol geautoriseerd is. Applicaties die dit succesvol ondersteunen zijn geen gemeengoed gebleken bij de HAN. Het is op dit moment niet duidelijk of het aanbod in de markt voor dit soort proces flow-ondersteuning laag is. Dit beleid staat daarom ter discussie.

5.2 Aanvraag HANaccount rol Student

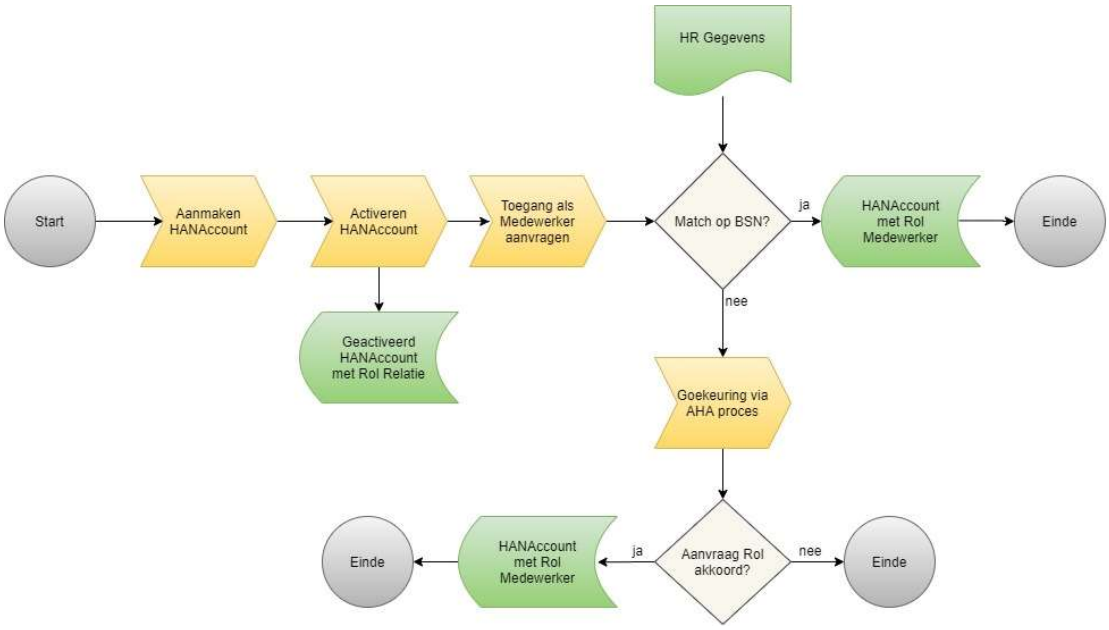
De procesflow voor een student om zelf een HANaccount aan te maken en die vervolgens op te waarderen naar de rol Student loopt als volgt (Figuur 15):



Figuur 15: procesflow opwaarderen rol Student

5.3 Aanvraag HANaccount rol Medewerker

De procesflow voor een medewerker (intern of extern) om zelf een HANaccount aan te maken en die vervolgens op te waarderen naar de rol Medewerker loopt als volgt (Figuur 16):

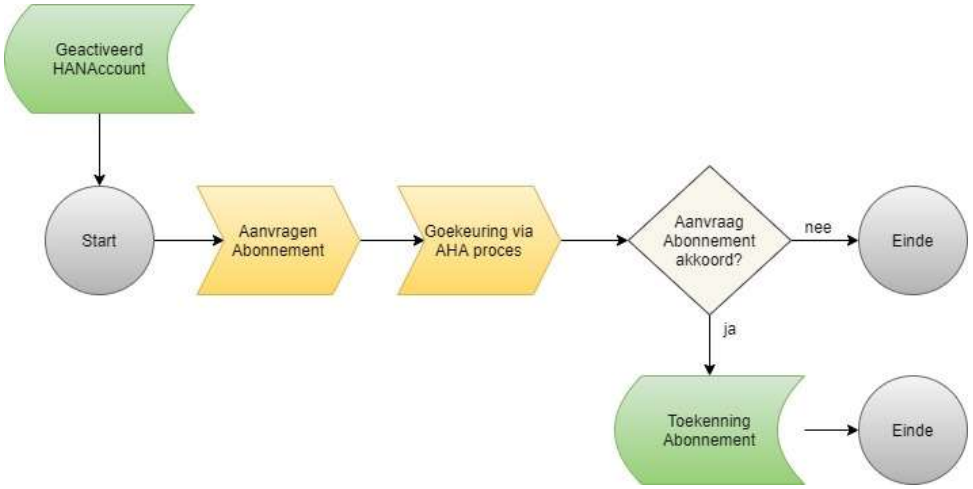


Figuur 16: Procesflow opwaarderen rol Medewerker

Het schema in Figuur 16 laat de procesflow zien voor zowel interne als externe medewerkers. Normaliter is na een verwerking van nieuw personeel in loondienst de centrale data store (IMAO) bijgewerkt waardoor het automatisch opwaarderen zal slagen. In de praktijk blijkt dat nieuwe medewerkers proactief hun HANaccount aanmaken waarbij het automatisch opwaarderen nog niet lukt omdat de juiste gegevens nog niet verwerkt zijn in het eHRM systeem. In dat geval zal een nieuwe interne medewerker hetzelfde proces doorlopen als een nieuwe externe medewerker. Deze vraagt toegang aan als medewerker en geeft daarbij het organisatieonderdeel op en een contactpersoon van de HAN. De gemandateerde persoon in de AHA applicatie kan hiermee beoordelen of de toegangsaanvraag terecht is of niet; goedkeuren, afwijzen of doorzetten naar een ander organisatieonderdeel.

5.4 Proces aanvragen abonnement

De procesflow voor het aanvragen van een abonnement is identiek aan de wijze waarop dit verloopt voor externe medewerkers (Figuur 17). Echter vraagt de persoon dan niet toegang aan als medewerker, maar tot een bepaalde dienst. Ook hierbij wordt een organisatieonderdeel en een HAN contactpersoon opgegeven en kan een gemandateerde persoon in de AHA applicatie de aanvraag goedkeuren, afkeuren of doorzetten naar een ander organisatieonderdeel.



Figuur 17: Procesflow aanvragen abonnement

5.5 Matrix rol en abonnementsamenstelling

Per rol zijn er een aantal abonnementen standaard (S), facultatief (F) of niet mogelijk (N) (zie Tabel 9):

FB via	SZ	ICT	ICT	ICT	ICT	MCV	O&O	SZ	Autotech	SZ	MCV	MCV	ICT	SZ	Educatie
	Abonnement														
	DLWO	Inloggen STAFF	inloggen STUD	Wifi wireless	Surfspot	Insite	Video	Alluris	EPDM Autotechniek	Rosis	VOM	Webredactie	HANDIN	HelpdeskInterface	Studiecentra Digitale bronnen	BuroExtern
Rol																
Medewerker	S	S	n	S	S	S	S	S		F	n	F	S	F	S	F
Student	S	n	s	S	S	S	S	S		n	n	n	S	N	S	N
Cats cursist	S	n	s	S	S	S	S	S		n	n	n	S	N	S	N
Relatie	F	n	n	F	N	F	F	N	F	n	f	F	F	N	N	F
Stagebegeleider	S	n	?	n	n	n	n	N		n	n	n	F	N	F	N
VDO_ZDGGM	S	n	S	S	N	N	S	N		n	n	n	F	N	F	N
Aanmelder	n	n	n	S	n	S	n	n								

Tabel 9: Matrix rol en abonnement samenstelling

6 TOEKOMSTIGE ARCHITECTUUR (SOLL)

In het visiedocument “HAN IAM Landschap” dat geschreven is door Capitar Security (bijlage 4 bij marktconsultatie) is de gewenste toekomstige architectuur op hoofdlijnen beschreven. Voor deze fase van het project is deze beschrijving afdoende. Aan de hand van de marktconsultatie en voortschrijdend inzicht zal deze toekomstige architectuur op een later moment in meer detail worden uitgewerkt.

7 VERSCHILLENANALYSE (IST/SOLL)

De verschillenanalyse zal gemaakt volgens POLDAT[9] gemaakt worden wanneer het project in de fase voor de aanbesteding komt en zal daarna gedurende de uitvoering van het project uitgewerkt worden.

[9] https://en.wikipedia.org/wiki/POLDAT

8 ROADMAP

In het visiedocument “HAN IAM Visie” dat geschreven is door Capitar Security (bijlage 5 bij marktconsultatie) is een globale roadmap opgenomen. Hierin wordt een fasering voorgesteld voor de implementatie van het toekomstige IAM-systeem. Voor deze fase van het project is deze roadmap afdoende. Aan de hand van de marktconsultatie en voortschrijdend inzicht zal deze roadmap op een later moment in meer detail worden uitgewerkt.

9 BIJLAGEN

9.1 Uitwerking Relatie Projecten en Initiatieven

VERVANGEN HAN-CARD

Projectbeschrijving

In het project HAN-Card wordt de huidige fysieke HAN-Card vervangen door een digitale variant. De HAN-Card wordt gebruikt voor diverse voorzieningen waaronder de Koffiemachines, toegang tot de campus (slagbomen), toegang tot bepaalde ruimtes en voor de tentamens bij een aantal academies.

Relatie met huidig project

De HAN-Card wordt bij diverse processen en voorzieningen ingezet als identificatiemiddel en vormt daarmee een wezenlijk onderdeel van Identity en Access Management. De verwachting is dat de digitale HAN-Card tegelijk met het nieuwe Identity and Access Management systeem wordt geïmplementeerd. Afstemming tussen beide projecten is daarom belangrijk.

AANSLUITING SOC/SIEM BIJ SURF

Beschrijving

Verkenningstraject van de HAN om eventueel aan te sluiten bij de SURF diensten Security Operations Centre (SOC) en Security Information & Event Management (SIEM).

Relatie met huidig project

Informatie ophalen bij projectleden of SURF voor standaarden over uitwisselen gegevens tussen IAM-systeem en SOC/SIEM diensten.

KOPPELING SYSTEEM UITZENDKRACHTEN

Beschrijving

Aanbestedingstraject voor de levering van uitzendkrachten en werving en selectie van medewerkers tot en met schaal 9. Tevens wordt hiervoor een koppeling gerealiseerd tussen systeem van leverancier en het inkoopsysteem van de HAN.

Relatie met huidig project

Er wordt van uit gegaan dat eHRM het bronsysteem blijft voor medewerkersgegevens en dat de integratie en processen daar op in worden gericht. In dat geval is er geen relatie. Wanneer de integratie en processen zo worden ingericht dat IAM bij het integratievraagstuk betrokken raakt, is er op gegevens en procesniveau wel een relatie.

PNIL REGISTRATIE

Beschrijving

Onder architectuur brengen van de gegevensuitwisseling van systemen voor tijdelijke inhuur en de HAN integratielaag.

Relatie met huidig project

Er wordt van uit gegaan dat HR het bronsysteem blijft voor medewerkersgegevens en dat de integratie en processen daar op in worden gericht. In dat geval is er geen relatie. Wanneer de integratie en processen zo worden ingericht dat IAM bij het integratievraagstuk betrokken raakt, is er op gegevens en procesniveau wel een relatie.

TIJDSCHRIJF & BEHEER TOOL PNIL

Beschrijving

Er is op dit moment geen informatie rondom Beschrijving beschikbaar om te kunnen beoordelen welke relatie dit project heeft met IAM.

Relatie met huidig project

Onbekend, mogelijk in relatie met **Fout! Verwijzingsbron niet gevonden.** hierboven.

INRICHTEN NIEUWE STRUCTUUR AFRONDEN (HIVL)

Beschrijving

Ontwerpen en inrichten van de nieuwe organisatiestructuur.

Relatie met huidig project

Geen. Project is grotendeels afgerond. Wijzigingen voor IDM zijn doorgevoerd in het huidige systeem.

DOORONTWIKKELING SERVICE BUS (HIVL)

Beschrijving

Onder architectuur brengen van de gegevenskoppelingen tussen systemen. Deze worden daarbij stapsgewijs omgezet van een klassieke ETL-integratie naar een Service oriented integratielaag.

Relatie met huidig project

Om het nieuwe IAM aan te kunnen sluiten op de integratielaag moeten de relevante bedrijfsobjecten beschikbaar zijn op de integratielaag en dient er voldoende ontwikkelcapaciteit beschikbaar te zijn.

CODERINGEN HAN

Beschrijving

Binnen dit project wordt voor een aantal primaire bedrijfsobjecten een coderingsconventie afgesproken en worden de processen ingericht om deze conventie te handhaven. Het doel is om daarmee de integratie van systemen en de uniforme opzet van processen te ondersteunen.

Relatie met huidig project

Geen relatie op procesniveau. De bedrijfsobjecten waarvoor binnen de scope van het project afspraken worden gemaakt, zijn voor het IAM-systeem hooguit secundaire gegevens. Wijzigingen in deze gegevens worden overgenomen vanuit de Integratielaag of via een directe koppeling met een van de bronsystemen en zullen slechts in de vorm van attributen voor identiteiten beschikbaar zijn.

DOMEINARCHITECTUUR INTEGRATIELAAG

Beschrijving

Binnen dit traject wordt een domeinarchitectuur ontwikkeld voor de integratielaag van de HAN.

Relatie met huidig project

De Domeinarchitectuur wordt op dit moment ontwikkeld en kan nog van invloed zijn op hoe de HAN integratielaag wordt gerealiseerd. Relatie is op dit moment lastig te duiden en daardoor als beperkt aangenomen.

VERVOLG HGIO/HAN.NL/INSITE

Beschrijving

Doorontwikkeling design en functionaliteiten voor de HAN Gebruikers en Interactie Omgeving (HGIO).

Relatie met huidig project

Scope ligt voornamelijk op han.nl en HAN-insite. Er zou een relatie kunnen liggen op de Selfservice componenten van IAM en die binnen het HGIO-traject worden gerealiseerd. Afstemming op functionaliteiten en design is mogelijk gewenst (navraag doen bij DA en HGIO).

HAN4ME APP

Beschrijving

Samenvoegen functionaliteiten 2 Apps tot 1 en uitbreiden van gewenste functionaliteiten voor met name studenten.

Relatie met huidig project

Mogelijk een relatie met Selfservice Component van IAM en HAN4me. Afstemmen met DA en HAN4me traject.

EUROPESE AANBESTEDING AFDRUKFACILITEITEN

Beschrijving

Aanbesteding centrale en decentrale afdrukfaciliteiten.

Relatie met huidig project

Wanneer de toekomstige HAN-Card ook wordt ingezet voor de afdrukfaciliteiten ontstaat een integratievraagstuk. Deze kan in dat geval opgepakt worden binnen de scope van project HAN-Card.

SIS IMPLEMENTATIE

Beschrijving

Aanbesteding van een nieuw systeem voor de deelnemeradministratie (studenten en cursisten). Binnen scope vallen de aanschaf en implementatie van Aanmelden, Inschrijven en Uitschrijven (AIU), Studievolg en de Onderwijscatalogus.

Relatie met huidig project

Indien IAM rechtstreeks koppelt op dit systeem, hebben deze projecten een sterke relatie. Een extra risico vormt dan de gelijktijdige uitvoer van SIS en IAM. Indien het IAM-systeem koppelt via de integratielaag, is de relatie iets minder sterk en ligt die vooral bij de realisatie van de juiste mapping van de gegevensset voor uitwisseling op de Service Bus.

DIGITALE ONDERSTEUNING TENTAMENORGANISATIE

Beschrijving

Binnen dit project worden de processen rondom toets afnames gedigitaliseerd.

Relatie met huidig project

Wanneer de toekomstige HAN-Card wordt ingezet als (digitaal) identificatiemiddel voor tentamens, kan dit eventueel impact hebben op IAM.

ONLINE PROCTORING

Beschrijving

Dit betreft een onderzoek naar de kaders voor Online Proctoring bij de HAN indien een vorm van een lockdown als gevolg van COVID-19 de beoordeling van summatieve toetsing niet goed uitgevoerd kan worden.

Relatie met huidig project

Een goede identificatie en ondersteuning bij Online Proctoring van de juiste student met respect voor privacy en de juiste toegang kan gefaciliteerd worden door IAM.

DLWO 2021

Beschrijving

Dit is meer een programma dan een project; hier worden diverse trajecten uitgevoerd aangaande de (toekomstige) Digitale Leer- en Werkomgeving van de HAN.

Relatie met huidig project

Met name de eis op flexibilisering van het onderwijs over de instellingsgrenzen heen en het versterken van de driehoek Onderwijs, Onderzoek, Werkveld vormt een duidelijke driver voor functionaliteiten die in het IAM-systeem aanwezig moeten zijn. Deze zijn vertaald in het PvE.

DIGITALE TOETSING

Beschrijving

HAN-brede inrichting van toets processen en ondersteuning middels een beperkt aantal toets applicaties.

Relatie met huidig project

Wanneer de toekomstige HAN-Card wordt ingezet als (digitaal) identificatiemiddel voor tentamens, kan dit eventueel impact hebben op IAM.

VOORBEREIDING VERVANGEN ONLINE LEEROMGEVING (ONDERWIJSONLINE)

Beschrijving

Vervanging van de huidige Online distributie-/ leeromgeving van de HAN.

Relatie met huidig project

De scope van dit project moet nog helder worden. Indien ontwikkelingen als eduID en edubadges worden meegenomen, heeft dit impact op het IAM-project. Indien de leeromgeving wordt aanbesteed om met name de huidige functionaliteiten te vervangen, is er geen relatie.

ONTSLUITEN CRM LEADS VAN EN NAAR BRONSYSTEMEN

Beschrijving

Vanuit oogpunt van architectuur is gewenst (en besloten) dat de gegevens omtrent wervingen en open dagen moeten worden gesynchroniseerd met andere bronsystemen waaronder Measuremail (nieuwsbrieven), Summit (evenementen applicatie), Roxen (CMS-websites) en CRM.

Relatie met huidig project

Indien de scope beperkt blijft tot genoemde systemen, is er geen relatie met het IAM-project. De vraag is echter of binnen de scope niet ook het SIS systeem moet worden opgenomen omdat leads uiteindelijk ook student kunnen worden en sommige gegevens van de student dan feitelijk een ander bronsysteem hebben (CRM in plaats van nu SIS). Zeker wanneer gegevens vanuit SIS ook weer aan CRM worden toegevoegd, moet CRM voor bepaalde informatie rondom de deelnemer sterk als bron worden gepositioneerd.

Indien het SIS in de scope komt, krijgt het initiatief ook een relatie met IAM voor de gegevens van studenten en cursisten. Ook hier geldt echter weer dat wanneer de gegevens via de integratielaag worden afgenomen, de relatie minder sterk is dan wanneer een directe koppeling met het CRM wordt gerealiseerd.

OPEN UP
NEW HAN_UNIVERSITY OF APPLIED SCIENCES
HORIZONS.