HAN IAM Visie

Identity & Access Management voor de HAN

Versie	0.5
Datum	26-2-2020
Status	Concept

HAN_

Inhoudsopgave

Document historie

V	Datum	Reviewers	Opmerking
0.1	15 augustus 2019	Edwin Castelein	Eerste opzet
0.2	4 september 2019		Tweede opzet t.b.v. workshop
0.3	24 oktober 2019		Nieuwe opzet met eenvoudigere koppeling aan doelen
0.4	8 januari 2020		Redacties verwerkt
0.5	26 februari 2019		Inleiding / business case toegevoegd Toevoegen van relevante diensten en onderzoek van SURF Conclusie over IAM-componenten die relevant zijn voor de HAN toegevoegd PaaS/SaaS aanbevelingen toegevoegd Verduidelijking ABAC/RBAC discussie

HAN_

Inleiding

Verantwoording

Moderne IT-dienstverlening voor een hoger onderwijsinstelling vereist een hoge mate van veiligheid én een hoge mate van gebruiksvriendelijkheid. De veiligheid is van belang om bijvoorbeeld de continuïteit van het onderwijs te garanderen, de integriteit van de onderwijsresultaten te borgen, onderzoeksgegevens veilig te stellen en de privacy van alle gebruikers, studenten en medewerkers, zeker te kunnen stellen. De gebruiksvriendelijkheid betekent in de moderne tijd niet meer alleen dat eenvoudig in applicaties kan worden ingelogd en dat ze eenvoudig te gebruiken zijn, maar ook dat mobiele apparaten ondersteund worden, samenwerken binnen en buiten de eigen instelling wordt gefaciliteerd, studenten bij meerdere instellingen tegelijk onderwijs kunnen volgen en digitale diensten kunnen worden geleverd aan aankomende studenten en alumni. Daar komt bij dat applicatieplatformen, al dan niet in de cloud geïntegreerd moeten kunnen worden.

Identity & Access Management levert hierbij de lijm die veiligheid en gebruiksvriendelijkheid bij elkaar brengt. Moderne oplossingen hiervoor, mits organisatorisch goed ingebed, zorgen voor een adequate beveiliging van het inlogproces, gebruikersaccounts en de rechten die gebruikers nodig hebben, maar bieden tevens de mogelijkheid om – door samenwerkingen met andere onderwijsinstellingen en met bedrijven – zonder en grote beheerinspanning derden toegang te verlenen. Ze ondersteunen met best practices en standaarden het gebruik van accounts van de organisaties waarmee wordt samengewerkt, veilige multi-factor authenticatie, eenmalig inloggen over meerdere applicaties heen, veilig gebruik van koppelingen tussen (cloud) applicaties, een goed beheer van toegangsrechten en een geautomatiseerd beheer van wie er toegang heeft en wie niet op basis van de status van een persoon (in dienst, uit dienst, aankomende student, student, etc.). Moderne oplossingen voor Identity & Access Management sluiten ook goed aan bij de initiatieven van SURF, zoals SURFconext, SURFSecureID en eduID.

Voor beveiliging is goed Identity & Access Management cruciaal. De laatste jaren is het principe van *zero-trust* voor beveiliging in opmars. Dit wil zeggen dat je eigenlijk niets en niemand meer kan vertrouwen, ook de eigen gebruikers niet (als ze al te vertrouwen zijn, zijn zij het dan wel zelf?) en dat de klassieke maatregelen van firewalls en VPNs bij lange na niet meer voldoende zijn. Van alle extra maatregelen die genomen moeten worden geven de meeste analisten aan dat databeveiliging en Identity & Access Management het meest urgent zijn om in te voeren.

De HAN beschikt momenteel over een zelfgebouwd systeem voor Identity & Access Management dat is toegespitst op geautomatiseerd aanmaken van accounts (inclusief gebruikersnamen, wachtwoorden en emailadressen) en, zij het beperkt, toegangsrechten. Dit is in feite basaal Identity Management en vooral gericht op de eigen medewerkers en studenten. Hoewel het systeem goed werkt en voor de HAN zeer nuttig is om in- en uitstroom van medewerkers en vooral studenten voor de digitale dienstverlening te automatiseren, is het onvolledig voor de huidige tijd (vooral beveiligingsaspecten ontbreken), voldoet het niet aan de moderne standaarden en is er ook geen ontwikkelteam dat uitbreiding en continuïteit zou kunnen bieden. De markt biedt voldoende out-of-the-box software-oplossingen die deze tekortkomingen niet hebben. Gebruik hiervan zal over de lange termijn meer toekomstvast zijn en minder kosten met zich mee brengen.

De HAN heeft ook single sign-on ingericht dat gebruiksvriendelijke toegang verschaft.

Identity & Access Management bestaat uit meerdere functies, waarvan er nu maar enkele zijn geïmplementeerd. Uitbreiden van het huidige systeem met meer zelfbouw is niet aan te raden wegens de hoge kosten van het bouwen van die functies. Maar ook de onderhoudbaarheid van het huidige systeem is een issue als meer cloud applicaties, die een eigen koppelvlak hebben (API) worden aangesloten. Leveranciers passen die APIs geregeld aan of breiden ze uit,

waardoor het Identity & Access Managementsysteem ook moet worden aangepast. Leveranciers passen hun software automatisch aan voor de grotere cloudapplicaties. Dat zelf blijven doen kan een ook kostbare aangelegenheid worden.

Het advies is daarom om een geheel nieuw systeem te implementeren op basis van speciale Identity managementsoftware uit de markt of – waar mogelijk – op basis van een cloud dienst voor Identity & Access Management.

Inhoud van dit document

In het vervolg van dit document wordt eerst aangegeven welke functies 'het begrip' Identity & Access Management allemaal biedt en vervolgens wordt aangegeven welke van deze functies voor de HAN van belang zijn. Daarbij wordt gebruik gemaakt van de volgende doelstellingen van de HAN:

1. Student beter gezien en gehoord;
2. Versterken HAN-cultuur, professionals, governance en gewenst gedrag;
3. Slagvaardige organisatie;
4. Bijdragen aan levenlang leren.

en van de daarvan afgeleide IV-doelen:

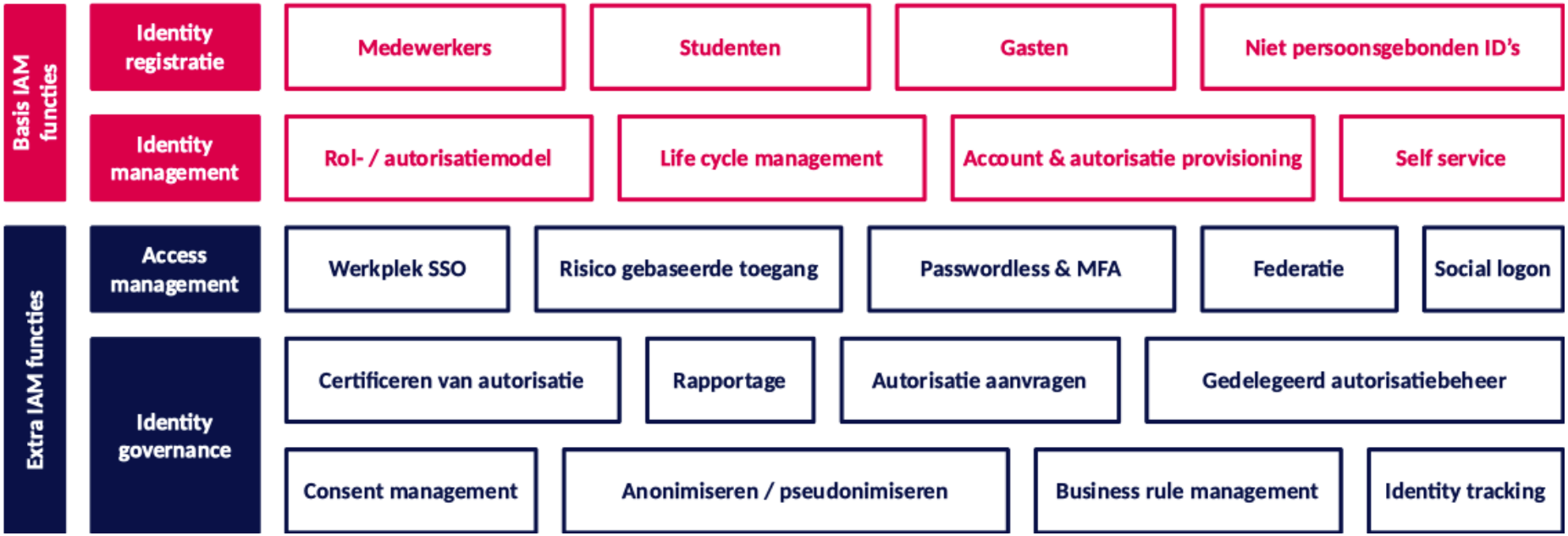
5. Gepersonaliseerd leren, onderzoeken en werken faciliteren;
6. Kwaliteit van gegevens en processen verbeteren;
7. Gegevens altijd toegankelijk voor studenten en andere belanghebbende;
8. Betrokken zijn in brede zin bij het professionaliseren van digitale vaardigheden.
9. Verder worden eerdergenoemde trends in het hoger onderwijs meegenomen.
   - Toenemend gebruik van mobiele apparaten;
   - Studeren bij meerdere instellingen;
   - Samenwerken over instellingen heen en met het bedrijfsleven;
   - Betere veiligheid bieden.

De relevante functies worden in een logische volgorde geplaatst zodat ze een roadmap vormen.

Behalve de relevante functies en in welke volgorde die geïmplementeerd kunnen worden, wordt ook aangeven welke functies uit de cloud beschikbaar zijn (IDaaS; Identity as a service) of als 'managed service' (PaaS; Platform as a Service).

In het vervolg van dit document spreken we niet meer over Identity & Access Management, maar kortheidshalve over *IAM*.

Overzicht over IAM-functies

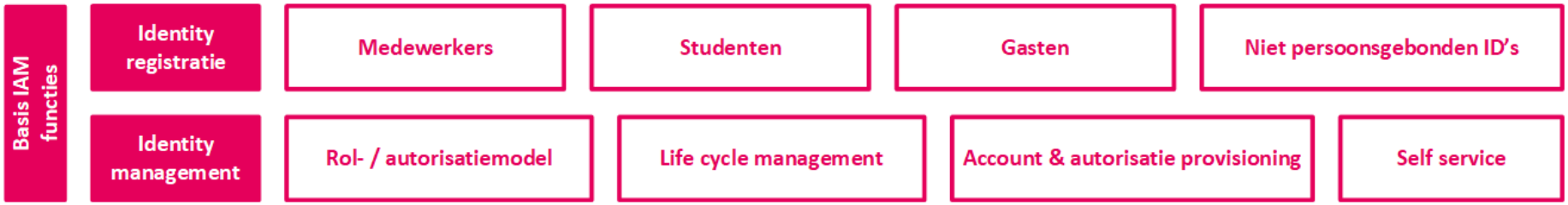


Toelichting bij het figuur

Het figuur hierboven geeft een schematisch overzicht van Identity & Access Management, zoals Capitar Security dat ziet. Het is opgedeeld in hoofdfuncties (Identity registratie t/m Identity governance) en gedetailleerde functies (aan de rechterkant). In het volgende hoofdstuk worden de gedetailleerde functies verder uitgediept. Daarna gaan we in op hoe deze zich verhouden tot de doelen die de HAN zich stelt. Daarmee wordt duidelijk welke functionaliteiten het meest belangrijk zijn voor de HAN.

Op dit moment heeft de HAN van de basisfuncties *Identity management* en *Identity registratie* ingericht. Het laatste alleen voor medewerkers en studenten. Access management is gedeeltelijk ingericht.

IAM-functies uitgewerkt



Identity registratie

Registratie van medewerkers, studenten, gasten, etc.

De registratie van personen gebeurt in huis (bijvoorbeeld bij HR of in een gastenportaal) of buiten de deur (bijvoorbeeld bij DUO of via een federatie of sociale netwerken). Bij elke registratie is van belang te weten wat de betrouwbaarheid ervan is (identiteitsbewijs geverifieerd, aangemeld via email, etc.). De betrouwbaarheid weegt mee bij het bepalen van de mate van toegang die een persoon krijgt.

Bij de registratie worden kenmerken vastgelegd van een identiteit, zoals functie, locatie, organisatieonderdeel, etc. Deze kenmerken noemen we *attributen*. De attributen worden gebruikt het bepalen van de toegang.

Verschillende registraties kunnen worden gecombineerd zodat personen die bijvoorbeeld zowel student als medewerker zijn, één identiteit krijgen. Ze krijgen dan om praktische redenen vaak wel verschillende accounts (voor student en medewerker). Zie bij Identity Management: Account & autorisatie provisioning.

In de toekomst kan het registratieproces gemakkelijker worden door dit *remote* te doen[1]. Dit kan worden gekoppeld aan de self service van een modern IAM-systeem.

Registratie van niet persoonsgebonden ID's

Niet persoonsgebonden ID's zijn identiteiten van groepen (bijvoorbeeld een secretariaat) of van apparaten. Ook hier moet de betrouwbaarheid worden bepaald om toegang te kunnen bepalen. Het kan nodig zijn om een verantwoordelijke identiteit (van een persoon) aan te stellen voor een groep of een apparaat en goed te definiëren wat er gebeurt als de verantwoordelijke persoon van functie verandert of weg gaat. Ook aan deze identiteiten kunnen attributen worden toegekend ten behoeve van het bepalen van toegang.

Identity Management

Rol- / autorisatie-model

Het is van belang om vast te leggen op basis van welke attributen identiteiten toegang krijgen tot IT-applicaties of onderdelen van applicaties (*autorisaties*). Als bij een attribuut meerdere autorisaties horen noemt men zo'n attribuut ook wel een *rol*. (Een voorbeeld is het attribuut 'student'. Een student krijgt toegang tot email, een ELO, etc.; dan wordt vaak gesproken over de rol 'student'.) Soms is het efficiënt om meerdere attributen te groeperen tot één rol. In bijlage 2 worden de twee methoden voor het bepalen van autorisatie besproken.

[1] Zie dit artikel van SURF: https://communities.surf.nl/artikel/remote-vetting-voor-surfsecureid

Life cycle management

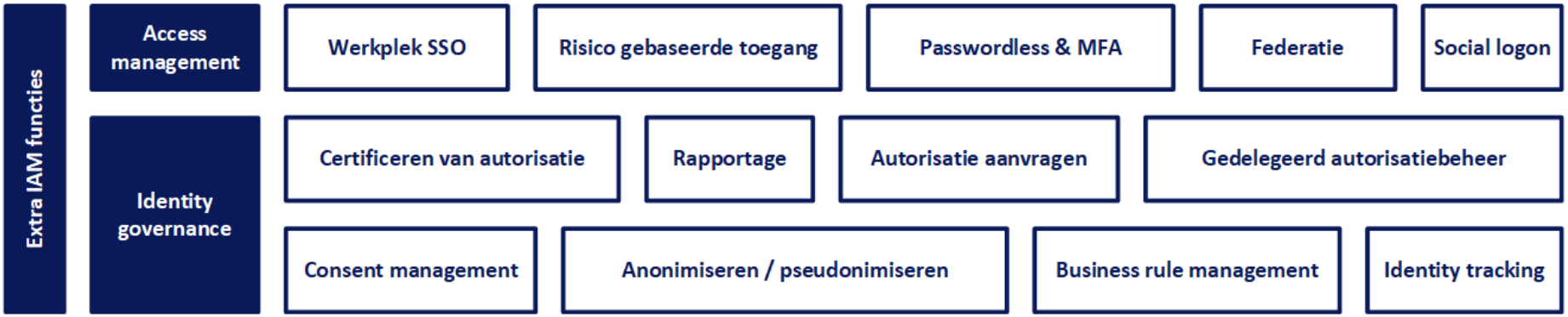
Het life cycle management geeft aan wat er moet gebeuren, als de status of functie van een identiteit wijzigt (van inschrijver naar student, van in dienst naar uit dienst, nieuwe functie, etc.).

Account & autorisatie provisioning

Account & autorisatie provisioning zorgt ervoor dat op basis van het rol-/autorisatie-model en het life cycle management de bij een identiteit horende persoon accounts en autorisaties krijgt in applicaties. Het zorgt er ook voor dat dit wijzigt op basis van het life cycle management.
De provisioning kan ervoor zorgen dat een persoon in alle applicaties hetzelfde wachtwoord kan gebruiken (single logon), maar dat is geen vereiste. Single sign on (SSO) kan ervoor zorgen dat een persoon überhaupt maar één keer hoeft in te loggen, maar daar is niet voor nodig dat het wachtwoord overal hetzelfde is. De implementatie hiervan is wel eenvoudiger als de gebruikersnaam hetzelfde is.
Een persoon die in meerdere registraties voorkomt, bijvoorbeeld zowel student als medewerkers is, krijgt vaak in één applicatie twee accounts. Dat komt omdat applicaties anders niet goed met de toegekende rechten om kunnen gaan.

Self service

Dit is met name bedoeld voor wachtwoord wijzigen en wachtwoord reset. Het kan ook worden gebruikt om gebruikers zelf gegevens (attributen) te laten beheren. Zoals een mobiel telefoonnummer.



Access Management

Werkplek SSO

Single SignOn voor het instellingsnetwerk.

Risicogebaseerde toegang

Dit is een vorm van beveiligde toegang die verder gaat dan alleen gebruikersnaam en wachtwoord. Er wordt vaak gebruikt gemaakt van machine learning om te bepalen wanneer een inlogpoging afwijkt van wat gebruikelijk is en dan kan toegang worden geweigerd of een extra inlogmiddel worden vereist (step-up authenticatie). Afgezien van machine learning kan ook gedrag worden afgedwongen, zoals dat alleen vanaf bepaalde locaties of met bepaalde apparaten of op bepaalde tijden mag worden ingelogd.

Federatie

Federatie wordt gebruikt voor SSO tussen webapplicaties en overstijgt daarmee het lokale netwerk. Het wordt vaak gebruikt in combinatie met lokale SSO. Gebruikers kunnen doen na het inloggen op het Windows netwerk zonder extra inlogmomenten ook inloggen op applicaties van bijvoorbeeld collega hogescholen.

Federatie heeft tevens de mogelijkheid om attributen mee te geven op basis waarvan autorisaties kunnen worden bepaald. Als er dan een rol-/autorisatie-model is, hoeven de autorisaties niet worden geprovisioned, maar worden ze gezet met behulp van de federatieve koppeling. Deze is vaak eenvoudiger te maken dan een provisioning koppeling.
Bij federatie ten behoeve van applicaties die door externen worden gebruikt wordt de registratie van identiteiten gedaan door een externe partij. Het is goed om dan in een contract de betrouwbaarheid van die registratie vast te leggen en de toegang navenant te bepalen.
In het hoger onderwijs is SURFconext populair om via één federatieve koppeling de eigen gebruikers toegang te verschaffen tot meerdere externe applicaties, of om andere gebruikers in het hoger onderwijs tot de eigen applicaties toegang te geven. SURF levert daarbij een dienst die het mogelijk maakt om alleen bepaalde groepen toegang te geven tot externe applicaties[2]. Daarnaast kan SURFconext indien gewenst ook extra attributen gebruiken uit externe bronnen[3].

Passwordless & MFA

Er wordt meer en meer gebruik gemaakt van nieuwe methoden om personen te authentiseren. De traditionele gebruikersnaam/wachtwoord combinatie wordt meer en meer vervangen door andere authenticatiemiddelen als apps op smartphones, gedrags- en gezichtsherkenning en tokens. Op dit moment worden deze methoden voornamelijk gebruikt als tweede factor naast een wachtwoord. Voor het hoger onderwijs stelt SURF SURFsecureID beschikbaar[4]. Dat vraagt wel om een goede registratie van gebruikers. Het is ook te gebruiken met de tokens van Microsoft.

Social logon

Deze term wordt gebruikt voor federatief inloggen via een social media partij (Facebook, Twitter, LinkedIn, etc.) of externe serviceprovider (Microsoft, Google, Apple). Deze partijen ondersteunen de moderne standaarden voor federatie, maar geven geen garanties over de betrouwbaarheid van de registratie. Het kan worden gebruikt om bijvoorbeeld aankomende studenten toegang te verschaffen tot informatie.

Identity governance

Certificeren van autorisatie

Dit is een middel om managers (of andere gedelegeerden, zoals applicatie-eigenaren) de rechten van personen te laten beoordelen en waar nodig te laten corrigeren. Dit gebeurt dan vaak periodiek. Behalve voor het bewaken van vertrouwelijkheid en integriteit wordt het ook vaak ingezet om kosten in de hand te houden als onderdeel van licentiemanagement.

Rapportage

Rapportages over wie wat mag worden vaak ingezet om aan een auditor aan te tonen dat er grip is op de toegang tot applicaties. Een andere belangrijke rapportage gaat over wie welke toegang heeft goedgekeurd. Deze kan worden gemaakt als *autorisatie aanvragen* of *gedelegeerd beheer voor autorisatie* worden gebruikt.

Autorisatie aanvragen

Hiermee kunnen gebruikers een rol of extra 'losse' autorisaties aanvragen. Het idee is dat dit wordt vastgelegd en erover wordt gerapporteerd. In de rapportage staat dan wie wat wanneer heeft aangevraagd en wie dat heeft goedgekeurd. Goedkeuring kan ook tijdelijk zijn.

Gedelegeerd autorisatiebeheer

In feite kan hiermee hetzelfde als met autorisatie aanvragen, behalve dat aanvragen niet nodig is. Een ServiceDesk kan dit gebruiken om een gebruiker snel

[2] Zie https://communities.surf.nl/artikel/surfconext-diensten-beschikbaar-maken-voor-een-beperkte-groep-gebruikers
[3] Zie https://communities.surf.nl/artikel/verrijk-je-identiteit-attribuutaggregatie-in-surfconext
[4] https://www.surf.nl/surfsecureid-beveilig-je-diensten-extra-met-tweefactorauthenticatie

extra autorisaties te geven. Een applicatiebeheerder om naast de autorisaties die al worden geprovisioned extra autorisaties toe te voegen voor sommige personen.

Privacybescherming / Consent management

Sinds de invoering van GDPR in Europa is *customer identity & access management* (CIAM) in opkomst. Het gaat dan om specifieke toepassingen die zorgen dat alleen attributen worden doorgestuurd naar een applicatie waarvoor de gebruiker toestemming (consent) heeft gegeven. Vanuit de academische wereld is IRMA een initiatief met dit oogmerk. Deze wordt ook gebruikt door SURF en is voor het Hoger Onderwijs een interessante optie.

Anonimiseren / pseudonimiseren

Bij governance hoort het netjes omgaan met gegevens. Indien een IAM-systeem een testversie heeft, dan verdient het in de meeste gevallen aanbeveling om namen en wachtwoorden te wijzigen. Anonimiseren betekent dat de gegevens worden gewijzigd en pseudonimiseren dat ze wel worden gewijzigd, maar dat de syntax intact blijft, zodat het systeem goed blijft werken.
Pseudonimiseren kan ook worden gebruikt bij federatief identity management, om wel geautoriseerd te worden voor een dienst, maar anoniem te blijven. Een voorbeeld is *Sign in with Apple*, waarbij de gebruiker zich bij een dienst kan authentiseren met een Apple ID, maar de keuze heeft om een applicatiespecifiek emailadres mee te geven in plaats van het eigenlijke emailadres.

Business rule management

Dit is het beheer van de regels die gelden voor automatisch toekennen van rollen en rechten. Identity governance kan een overzicht geven van rollen en rechten van identiteiten, maar het is net zo belangrijk om te weten hoe die tot stand komen en evt. wie toekenning heeft goedgekeurd.

Identity tracking

Met Identity tracking is het mogelijk om de activiteiten van identiteiten in de gaten te houden en met name activiteiten die afwijken van het gangbare gedrag. Het gaat dan natuurlijk om inlogacties, maar eventueel ook gebruik van autorisaties. Toegepast voor autorisaties op een file server kun je hiermee bijvoorbeeld sneller ransomware ontdekken.

De HAN-doelen en de IAM-functionaliteiten

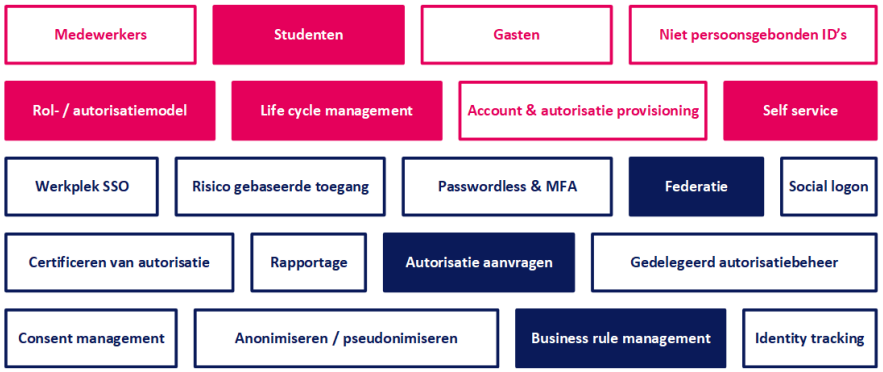
De missie van de HAN is tweeledig:

- Het kwalificeren, socialiseren en vormen van studenten voor toekomstige beroepspraktijk en burgerschap
- Het leveren van innovaties in een dynamische, globaliserende en complexe samenleving

Vanuit deze missie heeft de HAN een aantal algemene doelen en een aantal IV-doelen gedefinieerd. Hieronder zal per doel worden aangegeven welke IAM-functies dat doel het meest ondersteunen.

HAN-doelen

1. Student beter gezien en gehoord

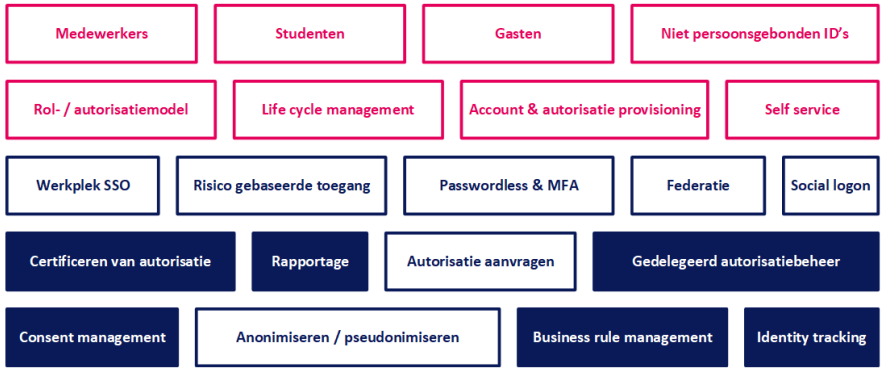


Om de student beter te faciliteren in zijn leerweg is het van belang dat zij of hij meteen bij aanvang van een studie of een vak de basisrechten heeft en dat het aanvragen van extra rechten via self service eenvoudig en 'near real time' gaat.

Voor studenten van andere instellingen is het van belang dat zij, gebruikmakend van de eigen digitale identiteit de juiste beperkte toegang kunnen krijgen (federatie).

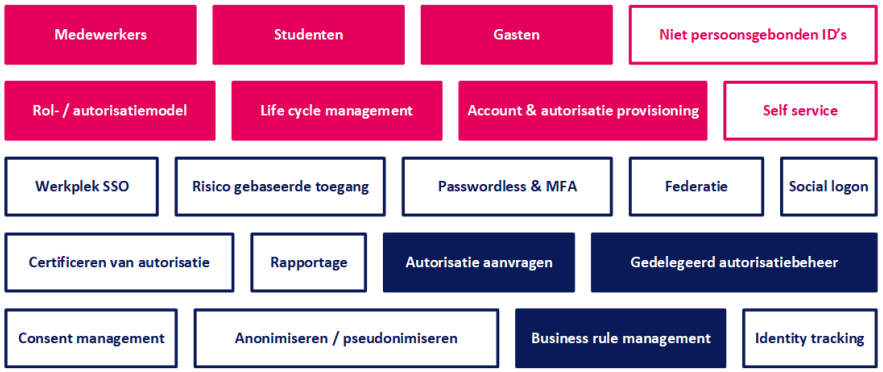
Om dit proces goed te monitoren moeten de business rules voor uitdelen van rechten goed kunnen worden beheerd.

2. Versterken HAN-cultuur, professionals, governance en gewenst gedrag



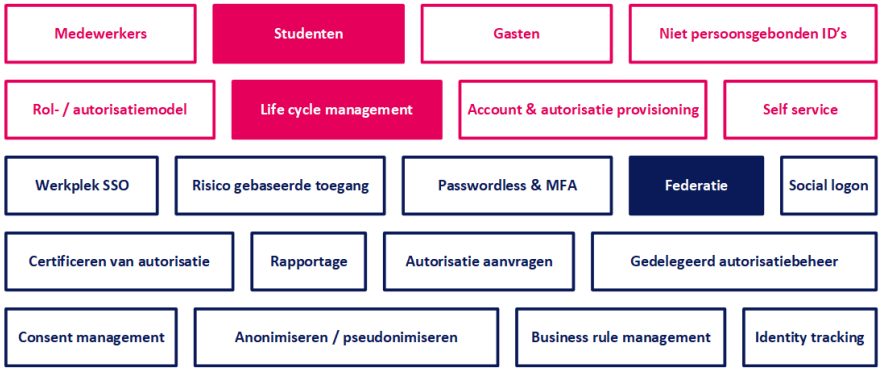
Professioneel gedrag vraagt erom dat de benodigde informatie beschikbaar is om besluiten te kunnen nemen en de juiste maatregelen vast te stellen. Voor IAM ligt dan de focus op het identity governance waarmee ervoor gezorgd kan worden dat de medewerkers de juiste dingen kunnen en de juiste keuzes maken.

3. Slagvaardige organisatie



Een slagvaardige organisatie vraagt om een slagvaardig IAM dat de basisfuncties op orde heeft zodat alle medewerker, studenten en gasten eenvoudig, snel en in verregaande mate geautomatiseerd rechten en toegang verkrijgen. Het aanvragen van extra toegang is optimaal ondersteunt. Business rules drijven IAM.

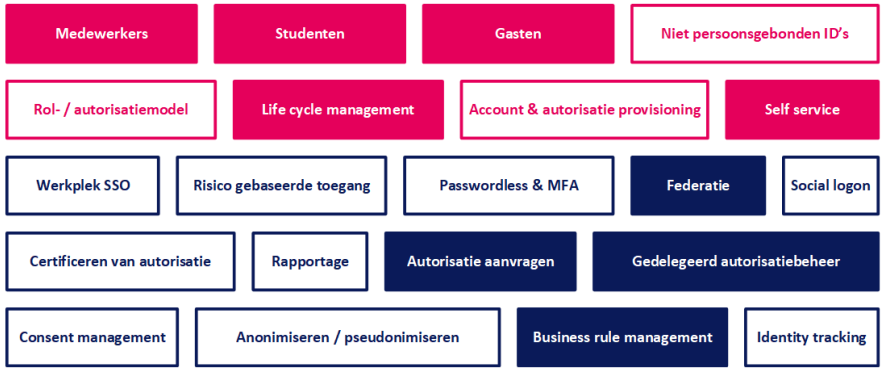
4. Bijdragen aan leven lang leren



Het bijhouden van de levensloop van een student, ook na zijn vertrek is de basis voor een optimale ondersteuning van levenslang leren. Ook het herkennen van studenten van andere instellingen, via federatie, draagt hieraan bij.

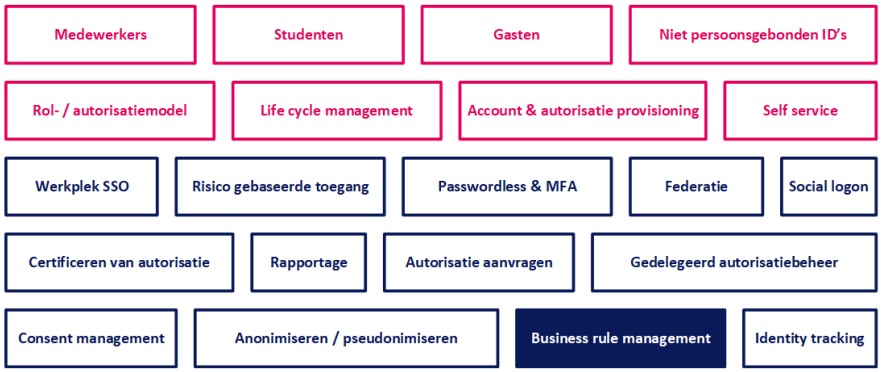
IV-doelen

5. Het gepersonaliseerd leren, onderzoeken en werken in het eigen netwerk van het individu faciliteren.



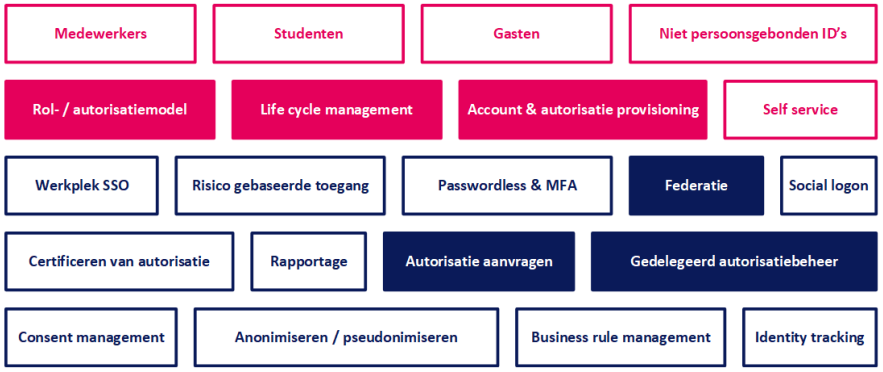
Goede registratie en life cycle management zorgt ervoor dat toegang tot informatie gepersonaliseerd kan plaatsvinden. Een goede gastenregistratie is noodzakelijk om het werkveld nauw te kunnen betrekken.

6. De kwaliteit van de gegevens en de inrichting van processen voor onderwijs, onderzoek en bedrijfsvoering verbeteren.



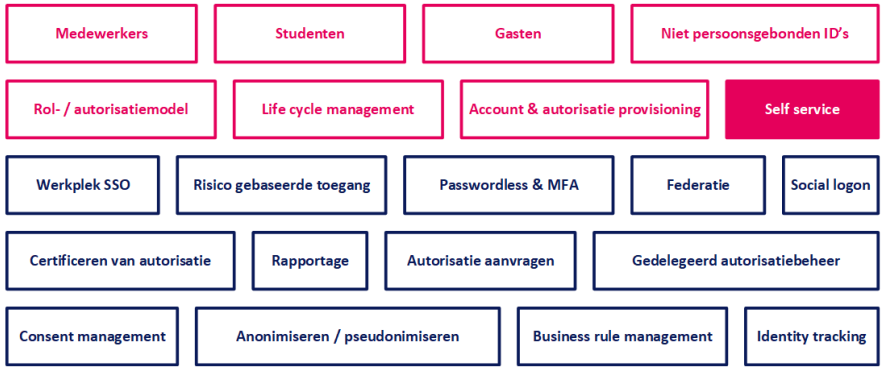
Algemeen gesproken kan je IAM zien als het automatiseren van bedrijfsprocessen. De directe bijdrage aan dit doel is echter beperkt.

7. De gegevens voor onderwijs en onderzoek en applicaties altijd toegankelijk en beschikbaar zijn voor studenten en andere belanghebbenden.



Door een goed rollenmodel, gekoppeld aan de levenslopen van de verschillende soorten identiteiten is informatie altijd beschikbaar op het juiste moment bij de juiste personen. Van belang is dat zowel de aanvraagprocessen als het provisionen van rechten goed is ingericht.

8. Alle betrokkenen in brede zin professionaliseren op het terrein van digitale- en informatievaardigheden.

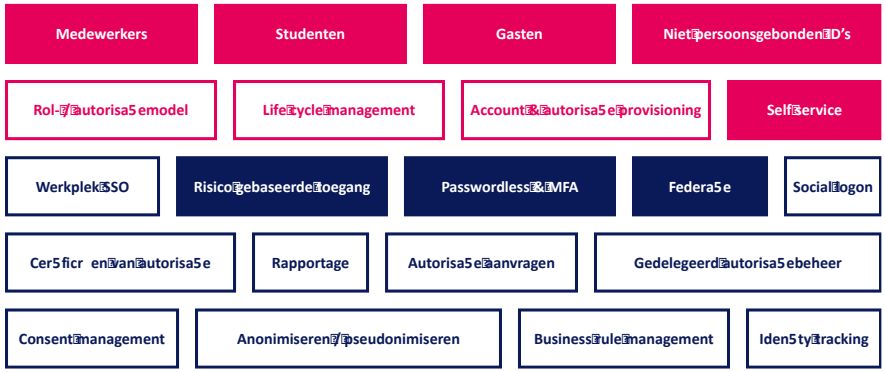


De Self service functie beoogt om de gebruiker zo zelfredzaam als mogelijk, en wenselijk, te maken.

HAN_

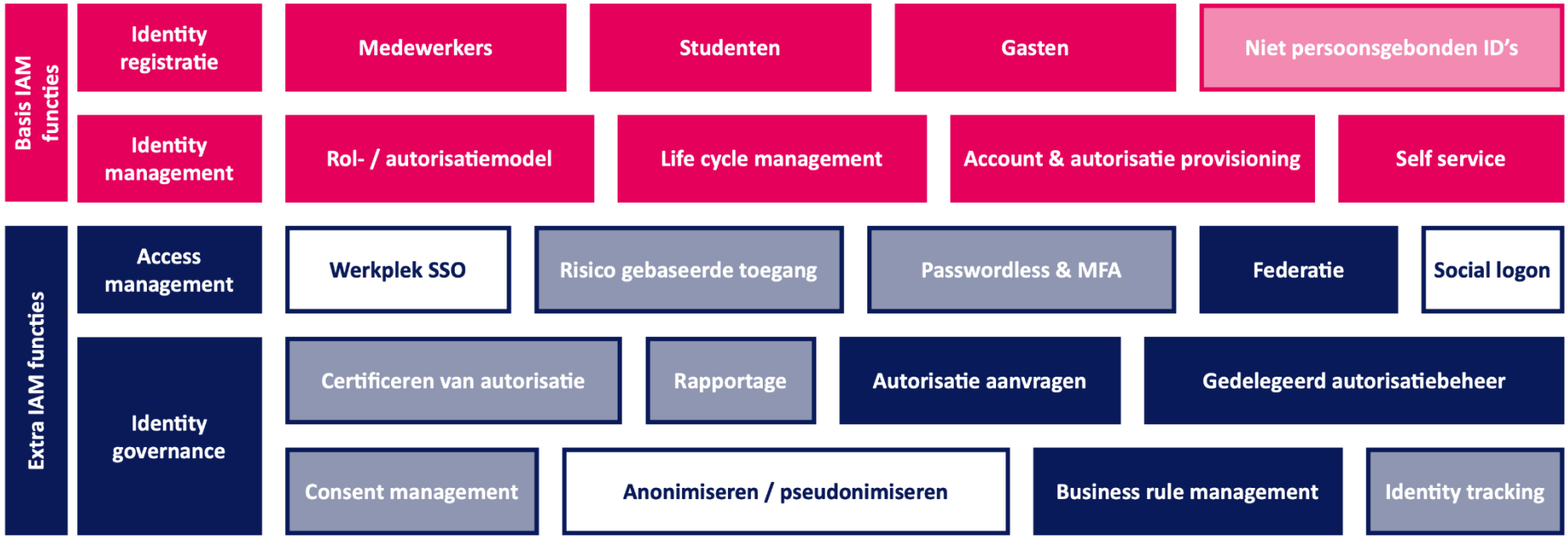
9. Trends

- Toenemend gebruik van mobiele apparaten;
- Studeren bij meerdere instellingen;
- Samenwerken over instellingen heen en met het bedrijfsleven;
- Betere veiligheid bieden.



Mobiele apparaten vragen om de modernste federatieve protocollen, zoals OpenID Connect en om goede beveiliging met risicogebaseerde toegang en MFA. Studeren bij meerdere instellingen vraagt om SURFconext en dus om federatie. Samenwerken vraagt ook om federatie en een betere overall beveiliging begint bij een goede registratie. Met name de verificatie van de gebruiker is dan van belang en het beheer van niet-persoonsgebonden accounts.

Noodzakelijke functionaliteiten en roadmap



De bovenstaande figuur laat zien welke functionaliteiten het meest voorkomen. De donker ingekleurde functies komen vaker voor, de licht ingekleurde functies slechts eenmaal en de niet ingekleurde functies komen niet voor.

Vier van de licht ingekleurde functies komen voor bij doel nummer 2 'Versterken HAN-cultuur, professionals, governance en gewenst gedrag', namelijk de licht ingekleurde functies bij Identity governance.

De overige drie komen alleen voor bij doel nummer 9, de trends. Ze hebben alle drie betrekking op een gedegen beveiliging (het laatste punt bij nummer 9) en dragen vooral bij aan het voldoen aan het *zero-trust* principe dat in de inleiding is genoemd. In het algemeen zijn ze eenvoudiger te realiseren dan de functies bij Identity governance. In een roadmap staan die laatste om die reden onderaan.

Roadmap

De roadmap voor de HAN, waar de basis IAM-functies en federatie al gedeeltelijk zijn ingevuld zal toch moeten starten met het opnieuw implementeren van die functies, omdat de huidige oplossing niet voldoet. Eerst extra functies creëren bovenop het bestaande fundament betekent dat die functies na de bouw van een nieuw fundament moeten worden gemigreerd, of erger, opnieuw moeten worden gebouwd.

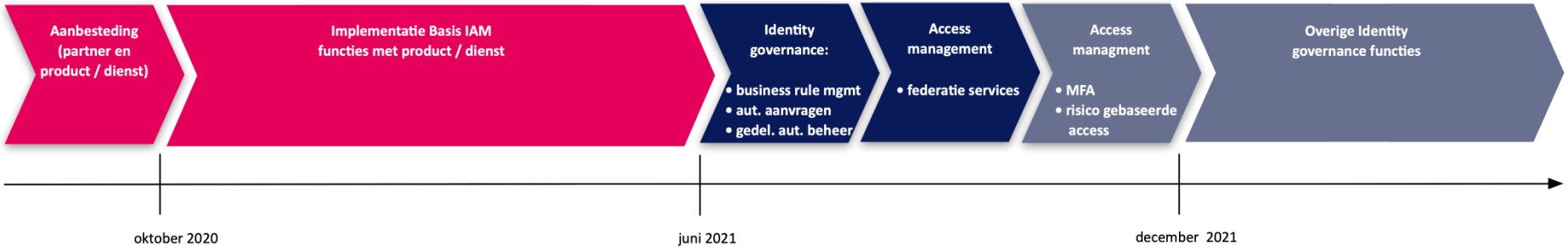
Voortborduren op het huidige systeem is niet haalbaar: er is momenteel geen ontwikkelteam dat verder kan bouwen aan wat al is gemaakt. De inschatting is dat er 3 tot 4 ontwikkelaars nodig zijn de komende twee jaar om dit systeem verder uit te bouwen. Het gaat dan om ontwikkelaars die kennis hebben van alle IAM-functies en de moderne standaarden. Als ze die kennis nog niet hebben, zijn er meer ontwikkelaars nodig of duurt het langer. Daarbij komt dat IAM-systemen moeten koppelen met andere applicaties en die wijzigen nogal eens. Er is dus nog een extra inspanning nodig al die wijzigingen op te vangen. Iets dat IAM-softwareleveranciers grotendeels al doen voor hun klanten. Daardoor zal de benodigde inspanning nog zeker 1 fte meer zijn.

Bovenstaande betekent dat de roadmap zal moeten beginnen met de bouw van de basis functionaliteit met een softwarepakket van een leverancier. Daaraan voorafgaand zijn echter twee zaken nodig:

1. Goede beschrijvingen van de processen rondom de functies die moeten worden gebouwd;
2. Technische uitwerking van die processen in termen van:
    a. de gegevensvelden die daarbij worden gebruikt;
    b. de logica die bij de functies wordt gebruikt;
    c. de standaarden, protocollen en beveiliging van de koppeling met andere systemen.

In een architectuurdocument[5] worden de procesbeschrijvingen uitgewerkt, maar bij de implementatie is de technische uitwerking nog een boel werk en die geldt ook per functie.

We komen zo tot de volgende roadmap:



Bij de implementatie en de daaropvolgende onderdelen van de roadmap is het zaak om eerst procesbeschrijvingen te maken (voor zover niet al aanwezig in het genoemde architectuurdocument) en daarna de technische uitwerking te maken.

[5] Bij dit document hoort een architectuurdocument waarin onder meer de processen zijn beschreven.

HAN_

IDaaS en PaaS opties

De trend voor IAM is dat er steeds meer Identity as a Service (IDaaS) aanbod in de markt is. Dit zijn standaard oplossingen voor IAM, waarbij de klant zich aanpast aan de mogelijkheden en bijbehorende processen van de leverancier.

Daarnaast is er ook aanbod van Platform as a Service (PaaS) oplossingen die dezelfde mogelijkheden bieden als on-premise oplossingen, maar vanuit de cloud worden geboden. Deze oplossingen stellen klanten veel meer in stata om hun eigen processen te automatiseren.

Voor de drie hoofdonderdelen van IAM geldt:

1. Access Management (MFA, web-SSO, federatie, etc.)
    1. er zijn IDaaS opties die prima werken voor alle organisaties, omdat er in het algemeen weinig maatwerk komt kijken bij deze functies. Voor integratie met de lokale Windows SSO is er vaak wel een kleine on-premise component;
    2. er zijn ook prima on-premise producten.
2. Identity Management (life cycle management, provisioning, etc.)
    1. IDaaS aanbiedingen zijn weinig flexibel en voor het hoger onderwijs meestal niet geschikt door de complexiteit van het life cycle management en van de provisioning;
    2. on-premise producten kunnen prima voldoen;
    3. het kan ook als PaaS worden afgenomen; dat voldoet ook prima.
3. Identity Governance
    1. IDaaS oplossingen voldoen meestal goed, maar omdat deze componenten het meest effectief zijn als ze samenwerken met identity management (die meestal on-premise of als PaaS worden gebruikt), zijn IDaaS oplossingen niet heel populair. Tenzij de klant echt alleen Governance wil inrichten (voor HO niet erg interessant).

Technisch beheer is altijd uit te besteden. Bij on-premise is het beheer wel zelf te doen, maar het is niet aan te bevelen wegens de specialistische kennis en de schaarste daarvan in de markt.

Functioneel beheer ligt altijd bij de klant. Wat hiervoor dient te worden ingericht is beschreven in een architectuurdocument[6].

[6] Bij dit document hoort een architectuurdocument waarin onder meer de organisatie rondom IAM is beschreven.

Bijlage I – Scope van IAM

Identiteiten

Er zijn vele personen die een rol binnen/relatie hebben met de HAN. In termen van IAM noemen we zo'n relatie een 'verbintenis'. Uitsluitend personen met een actieve verbintenis vallen onder de aansturing van IdM. Een persoon kan meerdere verbintenissen tegelijkertijd hebben met de HAN, bijvoorbeeld student en medewerker. We onderkennen de volgende verbintenissen:

Deelnemer

Individu die onderwijsactiviteiten afneemt bij de HAN

Interne Medewerker

Een individu dat een arbeidsovereenkomst heeft gesloten met de Stichting Hogeschool van Arnhem en Nijmegen

Relatie

Een verband tussen meestal twee (soms meerdere) individuen en/of organisatie(onderdelen)

Gast

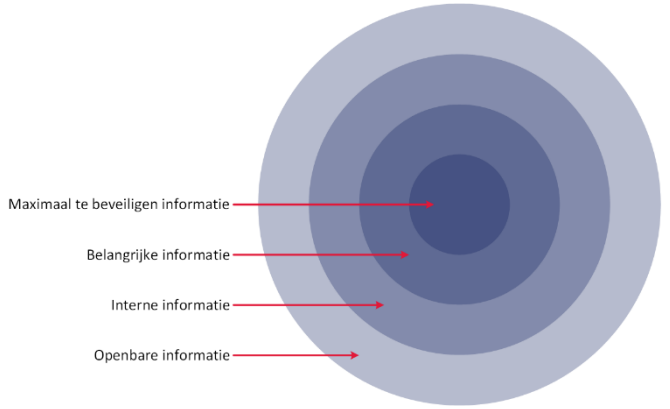
Dit zijn alle personen die niet in de bovenliggende categorieën vallen maar wel (beperkte) toegang tot informatie van de HAN nodig hebben. Voorbeelden hiervan zijn adviseursgastddocenten, vrijwilligers.

Buitenwereld

Dit zijn alle personen die ongeïdentificeerd informatie van de HAN gebruiken. Deze krijgen uitsluitend toegang tot de openbare informatie (zie volgende paragraaf) en vallen daarbij buiten de scope van IAM.

Informatie

Zoals in het figuur hieronder is aangegeven verdelen we informatie in vier klassen. In welke klasse informatie valt hangt onder andere af van de risico's de HAN loopt/wil lopen. Per klasse geldt een andere set van beveiligingsregels en daarmee ook een andere set van IdM- en AM-maatregelen.



Figuur 1 - Classificering van informatie

Maximaal te beveiligen informatie

Dit betreft informatie met een groot risico voor de HAN of personen gerelateerd aan de HAN. Vaak ingegeven door wet- en regelgeving, bijv. Persoonlijke Identificeerbare Informatie (PII), de AVG, beleid etc. Maar ook bepaalde financiële en strategische informatie valt hieronder.

Toegang tot deze informatie gaat op strikt persoonlijke basis en in de meeste gevallen is een dubbel authenticatie (naast gebruikersnaam en wachtwoord nog een derde factor) vereist.

Proces specifieke informatie

Dit is informatie die voor de ondersteuning van HAN-processen van belang zijn en toegankelijk voor specifieke groepen. Denk hierbij bijvoorbeeld aan studieresultaten of informatie van afdelingen waarop iemand niet werkzaam is. Toegang tot dergelijke informatie wordt beperkt op basis van je rol binnen de HAN. Hierbij moet de rol gezien worden als een combinatie van de verbintenis, de organisatie-eenheid (academie of afdeling) en verdere detaillering zoals bijvoorbeeld klas, werkgroep of team.

Interne informatie

Dit is informatie die voor eenieder binnen de HAN toegankelijk is, maar waarvoor de HAN wel zeker wil weten dat je een verbintenis hebt met de HAN. Met name generieke informatiediensten als wifi, het intranet of toegang tot Office365 horen hieronder. Toegang tot deze informatie is mogelijk voor iedereen die zich heeft geïdentificeerd bij de HAN.

Openbare informatie

Dit is de informatie die voor iedereen binnen en buiten de HAN toegankelijk is. De toegang tot deze informatie hoeft niet afgeschermd te worden en valt daarmee buiten de scope van IdM en AM.

HAN_

Bijlage II – Toelichting op rollen: RBAC of ABAC?

Er is in de markt veel discussie over het werken met rollen of in plaats daarvan met attributen. Er zijn aanhangers van role based access control (RBAC) en van attribute based access control (ABAC). Er is zoveel onduidelijkheid hierover dat het enige uitleg vereist. Dat gebeurt in deze bijlage.

RBAC houdt in dat de rechten in een of meerdere applicaties geaggregeerd worden in een rol. Een voorbeeld is dat de rol 'emeritus-hoogleraar' wordt gedefinieerd, waarbij alle rechten in verschillende applicaties worden aangegeven die iemand met deze rol moet/mag hebben. Als rollen *out of the blue* moeten worden bedacht zodat alle gebruikers minimaal één rol hebben, levert dat eenmalig een heleboel werk op, maar is ook het onderhoud van die rollen en de rechten die erbij horen erg veel werk. Daarom worden meestal bestaande gegevens gebruikt, zoals *medewerker met een bepaalde functie* en *student met studierichting* gebruikt. Deze volgen uit een HR-systeem en een SIS. Maar er kunnen ook aanvullende rollen worden bedacht die niet uit een systeem volgen. Denk daarbij aan taken die moeten worden uitgevoerd, maar die niet altijd aan een specifieke functie worden gekoppeld.

ABAC wordt ook wel *rule based access control* genoemd, omdat het de gegevens die bekend zijn over iemand (de attributen) met behulp van regels vertaalt naar wat die persoon mag: de rechten. Ook de rechten zijn weer attributen in deze theorie. Hierbij moeten dan eerder regels worden beheerd dan rollen. Voor externe personen die toegang krijgen is het lastig om rollen te definiëren en kun je beter uitgaan van de attributen die worden meegegeven. Dan ligt ABAC dus meer voor de hand.

Steeds vaker wordt in de markt geadviseerd om hybride access control te gebruiken, een mix van RBAC en ABAC. In feite is dat wat in de praktijk vaak gebeurt. Immers, als RBAC uitgaat van de gegevens in een HR-systeem of een SIS, kun je dat net zo goed ABAC noemen, want je maakt rollen van gegevens (attributen) uit die systemen. Je beheert ook eerder regels dan rollen in dat geval. Alleen de rollen die met taken te maken hebben zijn vaak niet af te leiden uit attributen. Maar de meeste organisaties definiëren slechts een zeer beperkt aantal *taakrollen*. Dat is ook niet nodig, als aanvullend op de beschikbare attributen die automatisch leiden tot rechten in applicaties de mogelijkheid wordt geboden om extra rechten aan te vragen en bij een aanvraag de opgave van de reden van de aanvraag verplicht te stellen. Sommige (of alle) aanvragen kun je ook eerst laten goedkeuren door een manager of applicatie eigenaar.

De meeste organisaties werken op deze manier, maar geven aan met RBAC te werken. In feite zouden ze net zo goed kunnen aangeven dat ze met ABAC werken.

Overigens maakt het voor het inzicht en overzicht over wie wat mag ook niet veel uit of RBAC of ABAC gebruikt wordt. En als aanvragen kunnen worden gedaan voor extra rechten, dan is het zaak die aanvragen en eventuele goedkeuringen te loggen en te laten bekijken door bijvoorbeeld managers. Daarmee is een groot deel van de governance meteen ingeregeld.