HAN Identiteiten architectuur

IAM-beleid, -landschap, -processen en functionele architectuur

Versie	0.5
Datum	juni 2020
Status	Concept
Auteurs	Steven van der Linden, René van Steenis, Peter Jurg

HAN_

Inhoudsopgave

Document historie

V	Datum	Reviewers	Opmerking
0.1	juni 2019	Patrick van Deijl, Edwin Castelijn, Michel Bekkers	Eerste opzet en, documentstructuur
0.2	september 2019		Opmerkingen reviewers verwerkt, aangepast naar opzet visie document
0.4	juni 2020		Organisatie beschreven
0.5	Juni 2020		User stories verder aangevuld

HAN_

Inleiding

Dit document beschrijft het Landschap van identiteitenbeheer (identity management - IdM) management en toegangsbeheer (access management - AM) voor de Hogeschool Arnhem Nijmegen (HAN).
Het is gebaseerd op de IAM visie zoals vast is gelegd in het document 'HAN IAM Visie'. De daarin vastgelegde visie is hierin uitgewerkt naar een werkbare situatie.

Documentstructuur

Als eerste zijn de algemene principes waaraan het IdM systeem dient te voldoen vastgelegd. Dit zijn vaststaande uitgangspunten.
In het tweede hoofdstuk is een globale weergave van het IAM-landschap gegeven, met daarin aangegeven de verschillende voor de HAN relevante componenten.
In hoofdstuk drie staat een overzicht van use cases, waarin de benodigde functionaliteit van een IAM omgeving voor de HAN is omschreven
Hoofdstuk vier beschrijft de IAM-processen welke aanwezig dienen te zijn om het identiteitenbeheer afdoende onder controle te hebben.
In het een-na-laatste hoofdstuk is de een functionele architectuur, met de verschillende functionele componenten, uitgewerkt.
Als laatste is een globale beschrijving van de benodigde IAM-organisatie beschreven.

HAN_

Gebruikte termen

De volgende IdM en AM specifieke termen worden gebruikt in dit document:

Authenticatiebeheer	Het proces van uitgeven en intrekken van authenticatiemiddelen aan een bestaande digitale identiteit. Dit betreft zowel gebruiksnaam/wachtwoord als multifactor-authenticatiemiddelen.
Autorisatie	Verlening van de bevoegdheid tot het verkrijgen van toegang (conform CDM)
Autorisatiebeheer	Het proces van uitgeven en intrekken van autorisaties aan een bestaande digitale identiteit. Dit kan op basis van de statuswijzigingen in de levenscyclus van de digitale identiteit en op basis van handmatige verzoeken.
Bronsysteem	Een informatiesysteem welke als betrouwbare bron wordt gebruikt voor het toekennen van aurtorisaties. Bij de HAN zijn de belangrijkste het HRM systeem ne het Studenten Administratie systeem
Digitale identiteit	Een digitale identiteit is de digitale vastlegging van gegevens welke gebruikt worden om vast te stellen wie de natuurlijk persoon is die gebruik maakt van toegangsrechten tot beveiligde informatie en/of beveiligde ruimtes en of deze natuurlijke persoon geautoriseerd is voor de verwerking die deze wil uitvoeren.
Doelsysteem	Een informatiesysteem waarvan de autorisatie is gekoppeld aan IdM. Dit houdt in dat aanpassingen in bronsystemene automatisch worden doorgevoerd in deze systemeen.
Functie	Het samenstel van werkzaamheden door de werknemer te verrichten volgens de door de werknemer met de werkgever gesloten arbeidsovereenkomst of door de externe werknemer met de opdrachtgever gesloten overeenkomst. (conform CDM)
Identiteitenbeheer	Het beheren van de levenscyclus van een digitale identiteit. Deze begint bij het creëren van een nieuwe identiteit en eindigt bij het archiveren ven een identiteit.
Permissie	De weergave van een autorisatie in een doelsysteem zoals het wordt vastgelegd in een IdM systeem. Over het algemeen een-op-een gekoppeld aan dat recht
PiL	Personeel in Loondienst: Een individu dat een arbeidsovereenkomst heeft gesloten met de Stichting Hogeschool van Arnhem en Nijmegen. (Conform ‘interne medewerker ‘ in CDM)
PNiL	Personeel Niet in Loondienst: Een individu dat werkzaamheden uitvoert voor de Stichting Hogeschool van Arnhem en Nijmegen anders dan op basis van een arbeidsovereenkomst. (Conform ‘externe medewerker ‘ in CDM)
Recht	Het recht binnen een doelsysteem.
Relatie	Een verband tussen meestal twee (soms meerdere) individuen en/of organisatie(onderdelen) (conform CDM)
Rol	Een bundeling van functionaliteiten waarvoor een individu is geautoriseerd (conform CDM)
Toegangsbeheer	Het proces van toegang geven tot informatiesystemen op basis van de aan een digitale identiteit toegekende autorisaties.
Verbintenis	De relatie die een digitale identiteit heeft met de HAN

HAN_

IdM en AM principes

Afgeleid van de hiervoor beschreven visie vormen de onderstaande principes het uitgangspunt voor een goed functionerend IdM en AM bij de HAN. Ongeacht de keuze voor de inrichting en of iets handmatig, procesmatig of geautomatiseerd dient te verlopen wordt voldaan aan deze principes.

Autoratieve bron identiteiten

Principe	Elke digitale identiteit is, via een registratie in een autoratieve bron, gekoppeld aan één natuurlijk persoon.
Uitleg	Een digitale identiteit komt voort uit een vastleggen van relevante gegevens van deze persoon in een registratiesysteem. De autoratieve bron[1] geldt als 'waarheid' voor alle handelingen en beslissingen die genomen worden bij het toekennen of intrekken van rechten aan die specifieke digitale identiteit.[2]
Onderbouwing	Juridisch moet elke transactie herleidbaar zijn naar één natuurlijk persoon. De autoratieve bron is de enige plek waar een relatie gelegd wordt tussen een natuurlijk persoon en een digitale identiteit.
HAN invulling	Voor deelnemers is dit de cursisten/studenten administratie (CATS). Voor medewerkers (PiL en PNiL) is dit de personeelsadministratie (eHRM). Voor relaties is dit het de rechtstreekse registratie in het IdM-systeem of het CRM systeem (…).

Levenscyclus identiteiten

Principe	Een digitale identiteit kent een vaste levenscyclus.
Uitleg	Het is te allen tijde inzichtelijk wat de status van een digitale identiteit is en wat de reden is waarom de identiteit die status heeft.
Onderbouwing	Zowel voor het toekennen en bewerken van roltoekenning als bij forensisch onderzoek achteraf is het noodzakelijk inzichtelijk te hebben wat de status van een digitale identiteit is en op welke momenten de status is veranderd. Dit om een verband te kunnen leggen tussen accounts in de logging van de onderzochte systemen en de natuurlijk persoon aan wie deze accounts toebehoord(e).
HAN invulling	De levensfasen die een digitale identiteit kent zijn: - Aangemaakt - Pre-actief (Grace voor) - Actief - Post actief (Grace na) - Gedeactiveerd - Gearchiveerd[3]

Account verantwoordelijke

Principe	Elk account, welke toegang geeft tot systemen of informatie van de HAN, is gekoppeld aan één digitale identiteit.
Uitleg	Voor elke account kan maar één persoon verantwoordelijk zijn. Niet meer en niet minder. De digitale identiteit is de verbinding tussen een account en een natuurlijk persoon.
Onderbouwing	Juridisch moet elke transactie herleidbaar zijn naar een natuurlijk persoon. Transacties uitgevoerd door accounts met meer dan één verantwoordelijke of geen verantwoordelijke voldoen hier niet aan.

[1] De autoratieve bron kan zowel een informatiesysteem van de HAN zijn als een vertrouwde bron buiten de Han, zoals bijvoorbeeld DigID.

[2] Het bronsysteem bevat vaak niet alle benodigde informatie. Deze kan later in het proces worden verkregen vanuit andere bronnen, worden gegenereerd door het IAM-systeem zelf of handmatig via het HAN-portaal worden ingevuld. Dit zijn echter niet de sleutel-attributen die een identiteit uniek maken.

[3] Een digitale identiteit wordt niet verwijderd, wel worden bij archivering alle niet noodzakelijke attributen geschoond. De identiteit blijft bestaan zodat, bij terugkeer van de persoon bij de HAN, de bijbehorende identiteit gereactiveerd kan worden.

HAN invulling | De medewerker, student en gast zijn zelf verantwoordelijk voor hun persoonlijke accounts.
Alle functionele-, systeem- of service-accounts hebben een eigenaar.

Eigenaar

Principe | Alle informatiesystemen die een impact hebben op het bedrijfsbelang en/of PII [4] -informatie bevatten of verwerken hebben een eigenaar.

Uitleg | Voor alle informatiesystemen binnen is een informatiesysteem-eigenaar toegekend welke de verantwoordelijkheid draagt voor het toegangsbeheer van de informatiesysteem.

Onderbouwing | Er moet één functionaris zijn die verantwoordelijk is voor de juiste toegang op het informatiesysteem. De uitvoering van taken kan gedelegeerd worden, maar de eindverantwoordelijkheid ligt in een hand. Dit ter voorkomen van conflicterende beslissingen.

HAN invulling | De eigenaar kan een proces-, systeem- of informatie-eigenaar zijn.

Roltoekenning

Principe | Bij de toekenning van rollen wordt van de volgende aspecten uitgegaan:
- Het risico wat aan een rol gekoppeld is.
- Het nut van de rol voor de identiteit

Uitleg | Of een digitale identiteit toegang tot een rol krijgt is primair afhankelijk van de risico's die de HAN, en de gekoppelde identiteit loopt als deze de rol toegekend krijgt. Daarnaast worden rollen alleen toegekend aan idetiteiten als deze toegevoegde waarde hebben voor die identiteit.

Onderbouwing | Risico-gedreven toegang is de basis voor de beveiliging; als er geen risico is hoeft het ook niet beveiligd te worden.
Het toekennen op basis van nut zorgt ervoor dat een identiteit niet allerlei toegang tot informatiesystemen krijgt die niet gebruikt gaan worden.

HAN invulling | Zie paragraaf Rollenmodel in hoofdstuk Identiteiten landschap.

Rolomschrijving

Principe | Rechten worden toegekend op basis van rollen met een functionele omschrijving.

Uitleg | Het toekennen, muteren en of intrekken van rechten geschiedt door middel van rollen welke voor aanvragers en goedkeurders te begrijpen zijn.

Onderbouwing | De goedkeurder is verantwoordelijk dat de juiste rechten worden toegekend. De functionele rollen geven een begrijpbare vertaling tussen systeemrechten en activiteiten. Dit stelt de direct leidinggevende in staat de juiste beslissing te nemen.[5]

HAN invulling | Zie paragraaf Rollenmodel in hoofdstuk Identiteiten landschap.

Proces Roltoewijzing

Principe | Toewijzen, muteren en intrekken van rollen loopt via een formeel en controleerbaar proces.

Uitleg | Door met controleerbare processen te werken, is geborgd dat rollen alleen worden toegekend of ingetrokken met goedkeuring van de juiste verantwoordelijke. Tevens moet het te allen tijde inzichtelijk zijn waarom een digitale identiteit een bepaalde rol heeft.

Onderbouwing | Alleen door op herhaalbare en gestandaardiseerde wijze te werken, is het mogelijk om controle te verkrijgen en te behouden. Tevens borgt dit de vastlegging van besluiten en beslissingen zodat achteraf traceerbaar is waarom een persoon een bepaalde rol heeft, of heeft gehad.

[4] PII, Persoonlijk Identificeerbare Informatie, de vastgelegde informatie van een natuurlijke persoon welke valt onder het regime van de AVG.

[5] Dit houdt niet in dat een goedkeurder elke aanvraag handmatig moet goedkeuren. Een rol kan worden automatisch toegekend op basis van eenmalig door de eigenaar vastgestelde toekenningsregels.

HAN_

HAN invulling	Zie hoofdstuk **Error! Not a valid result for table.**.

Proces Rechtentoewijzing

Principe	Toewijzen, muteren en intrekken van rechten aan rollen loopt via een formeel en controleerbaar proces.
Uitleg	Door met controleerbare processen te werken is geborgd dat rechten alleen aan rollen worden toegevoegd of ingetrokken met goedkeuring van de juiste verantwoordelijke. Tevens is het te allen tijde inzichtelijk waarom een rol een bepaald recht bevat.
Onderbouwing	Alleen door op herhaalbare en gestandaardiseerde wijze te werken, is het mogelijk om controle te verkrijgen en te behouden. Tevens borgt dit de vastlegging van besluiten en beslissingen zodat achteraf traceerbaar is waarom een rol een bepaald recht bevat, of heeft bevat.
HAN invulling	Zie hoofdstuk **Error! Not a valid result for table.**.

Autorisatiecontroles

Standaard	Toewijzing van rechten aan digitale identiteiten wordt op regelmatige basis aantoonbaar gecontroleerd.
Uitleg	Er moet op regelmatige basis worden gecontroleerd of de verleende autorisaties nog steeds nodig zijn.
Onderbouwing	Omdat het IT-landschap verandert, en dat er vergissingen kunnen worden gemaakt bij het handmatig uitdelen van rollen is het zaak dat er op regelmatige basis wordt gecontroleerd of er geen afwijkingen zijn tussen het rollenmodel en de werkelijkheid.
HAN invulling	?

Informatiesysteemwijzigingen

Principe	Bij installatie van nieuwe informatiesystemen en wijzigingen in bestaande informatiesystemen wordt de impact op de rollen beoordeeld en waar nodig actie ondernomen.
Uitleg	Bij alle wijzigingen in het informatiesysteemlandschap wordt in de impactanalyse gekeken of er impact is op de autorisaties en rollen. Voor nieuwe informatiesystemen betekent dat dat de autorisatie-structuur aansluit op het vastgestelde rollenmodel. Voor mutaties in bestaande informatiesystemen betekent dit dat de verandering wordt getoetst aan het autorisatiebeleid.
Onderbouwing	Het informatiesysteemlandschap staat niet stil. Bij elke wijziging kan er een risico worden ingebouwd.
HAN invulling	?

HAN_

Privacy by design

Principe	Privacy van personen waarvan gegevens worden vastgelegd in het IdM systeem worden zo veel mogelijk gewaarborgd door: ➢ Alleen een identiteit creëren als er een die een actieve verbintenis heeft. ➢ Alleen gegevens opslaan welke noodzakelijk zijn voor het uitgeven of intrekken van rechten. ➢ Alle gegevens kennen een vastgestelde bewaartermijn.
Uitleg	Door dit principe wordt zeker gesteld dat de gegevens welke worden gebruikt door het IdM proces voldoen aan de wet- en regelgeving op gebied van persoonsgegevens.
Onderbouwing	Een IdM systeem bevat Persoonlijke Identificeerbare Informatie welke valt onder het regime van de Algemene verordening gegevensbescherming (Avg).
HAN invulling	Standaard uitgangspunt voor alle Avg gevoelige informatiesystemen

Identiteiten landschap

De figuur hiernaast geeft het IAM-landschap van de HAN weer. Het legt uit hoe door middel van identificatie, authenticatie en autorisatie een natuurlijk persoon toegang krijgt tot de informatie die die persoon nodig heeft om conform zijn of haar verbintenis met de HAN.

Natuurlijk persoon

Alle toegang is ten behoeve van een natuurlijk persoon. Een natuurlijk persoon kan meerdere verbintenissen tegelijk hebben met de HAN.

Digitale identiteit

De digitale identiteit van een persoon is de sleutel tot alle zaken welke op digitaal gebied rondom de persoon geregeld wordt. Er zijn verschillende digitale identiteiten mogelijk. Eén natuurlijk persoon kan meerdere vormen van digitale identiteiten gebruiken om de HAN te benaderen, vanuit de HAN gezien zullen ze als aparte, niet gekoppelde identiteiten worden gezien.

HAN-identiteit

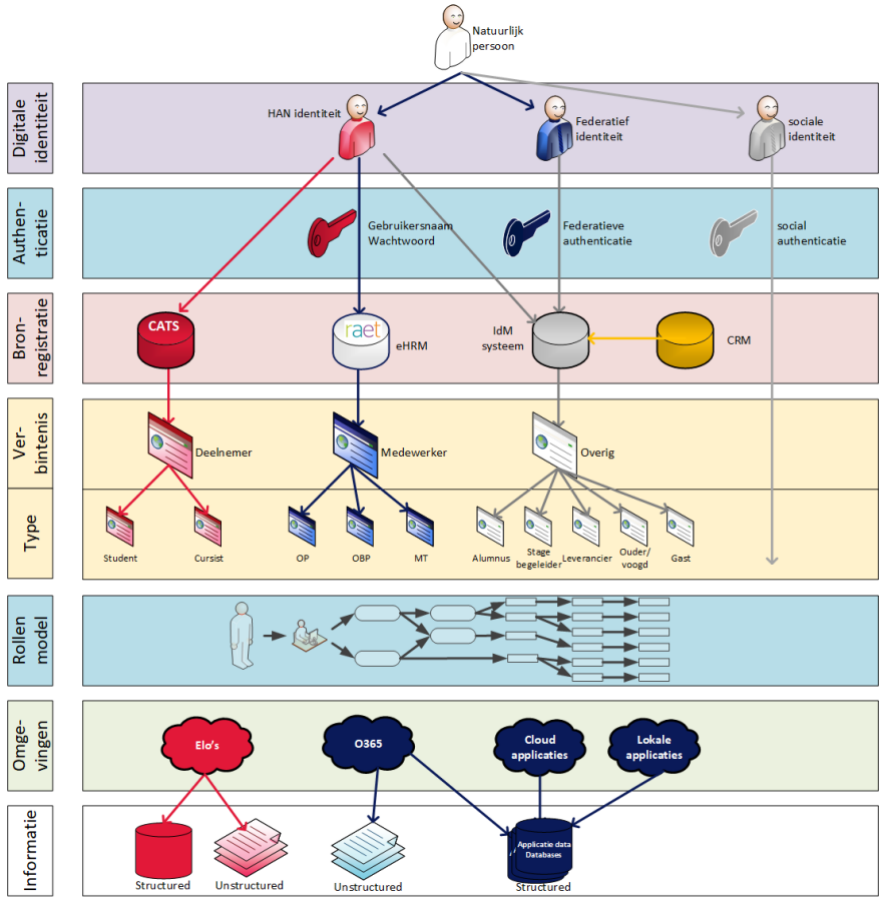
Dit is een identiteit welke volledig onder controle staat van de HAN. Deze wordt initieel aangemaakt via het HAN-portaal en daarop verrijkt met interne gegevens.

Federatieve identiteit

Dit is een identiteit die onder controle staat van een organisatie waarmee de HAN een vertrouwensband heeft op dit gebied. Hierbij kan bijvoorbeeld gedacht worden aan een andere onderwijsinstelling. Een persoon die aldaar een digitale identiteit heeft hoeft niet ook een identiteit binnen de HAN te hebben, alle informatie die noodzakelijk is, is via de vertrouwde relatie over te halen.
Voorbeelden hiervan zijn DigID of SURFconnext.

Sociale identiteit

Een sociale identiteit, een digitale identiteit gekoppeld aan een sociale media, zoals bijvoorbeeld een facebook-account, kan voor beperkte toegang gebruikt worden. De HAN kan de juistheid van zo'n sociale identiteit niet verifiëren, dus ook niet vertrouwen.



Authenticatie

Elke HAN-identiteit krijgt een eigen unieke gebruikersnaam/wachtwoord combinatie die de persoon zelf kan beheren via het HAN-portaal. Deze wordt gebruikt voor alle vormen van aanmelden.
Geaccepteerde federatieve identiteiten krijgen via hun eigen authenticatiemethode toegang.[6]
Sociale identiteiten krijgen via het authenticatiemiddel van hun sociale media toegang.[7]

Bronregistratie

Er zijn verschillende bronregistraties welke de informatie aanlevert over de specifieke verbintenis. Zoals begin- en einddatum, status, organisatieplaats/academie, type.
De bronregistratie bevat de enige waarheid over de verbintenis. Deze is sturend voor de bepaling welke rechten en toegang ene persoon krijgt bij de HAN.
Voor deelnemers is de bronregistratie CATS, voor medewerkers is dat RAET.
De bronregistratie voor de relaties is primair het identiteitensysteem zelf waarin de relaties rechtstreeks worden vastgelegd. Voor een deel van de relaties zou deze gevoed kunnen worden vanuit het CRM.
Naast de bronregistraties zijn er ook andere bronnen van informatie welke gebruikt kunnen worden voor het aanvullen van een digitale identiteit of het juist toekennen van rollen. Denk hier bijvoorbeeld aan de organisatie- of opleidingsstructuur.

Verbintenis

Welke relatie een natuurlijk persoon, via zijn digitale identiteit, heeft met de HAN wordt een verbintenis genoemd. Er zijn drie typen verbintenissen, met daaronder een aantal subverbintenissen.
Relaties welke niet leiden tot toegang tot informatiesystemen van de HAN worden buiten beschouwing gelaten.

Deelnemers

Alle identiteiten die een opleiding volgend bij de HAN hebben een verbintenis van dit type. De subverbintenissen zijn:
- Student
- Cursist

Medewerker

Alle identiteiten die een werkrelatie hebben met de HAN hebben een verbintenis van dit type. De subverbintenissen zijn:
- Onderwijzen Personeel (OP)
- Ondersteunend en Beherend Personeel (OBP)
- Management Team (MT)

Overig[8]

De volgende relaties worden binnen de HAN onderkend:
- Gast
- Werkgevers/stagebegeleider
- Leverancier
- Ouder/voogd

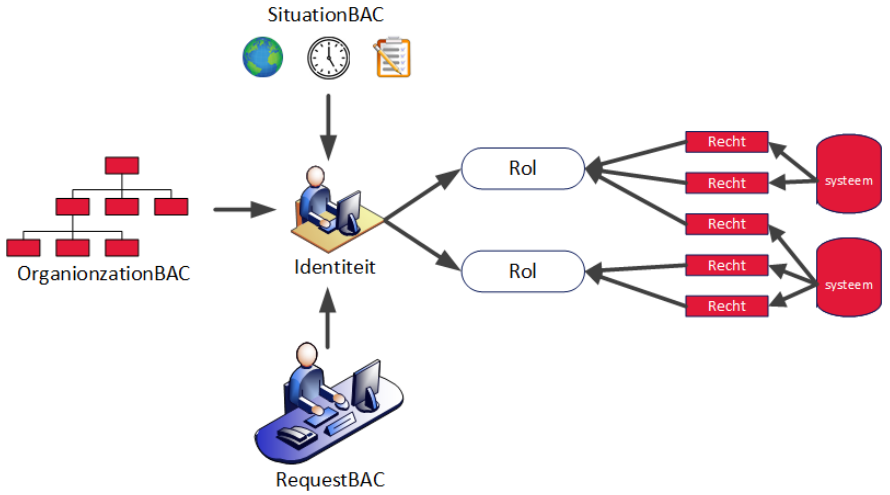
Nota bene: De basis voor de verdeling is het verschil in de bronsystemen, levenscyclus of de beheerprocessen. Alleen als die verschillen, is het van belang het als afzonderlijke verbintenis of subverbintenis te zien.
Nota bene: Het rollenmodel in de Enterprise Architectuur onderkent meer subverbintenissen. Deze leiden echter niet tot andere autorisaties en kunnen in het licht van IdM en AM buiten beschouwing gelaten worden. Zodra dit onderscheid wel ontstaat dient er een nieuwe subverbintenis te worden gedefinieerd binnen IdM en AM.

[6] Afhankelijk van de vertrouwensrelatie geeft een federatieve authenticatie meer of minder toegang.
[7] De toegangsrechten van sociale identiteiten zijn beperkt omdat er geen vertrouwensrelaties mogelijk is.
[8] In de huidige inrichting wordt hiervoor het woord ‘relatie’ gebruikt. Dit is echter verwarrend omdat deze term meerdere betekenissen kent binnen de HAN.

Rollenmodel

Rolconcepten

Er zijn verschillende manieren waarop een identiteit rollen kan toegewezen krijgen. In het figuur hiernaast staan de belangrijkste weergegeven.



De meeste toewijzingen zullen ‘statisch’ plaatsvinden op basis van de organisatieplaats van een identiteit. De toekenningscriteria zijn gebaseerd op gegevens uit een autoratief bronsysteem. Dit is een combinatie van de verbintenis plus een aantal andere statische attributen als faculteit, en functie of opleiding. Deze ‘Organizational based access (OBAC)’ wordt vaak Role Based Access (RBAC) genoemd. Over het algemeen wordt 80% van de rechten op deze basis toegekend.
Daarnaast worden ook rollen toegekend op basis van aanvragen (Request Based Access). Dit zijn de rollen waarvan de toekenningscriteria niet voortkomen uit een bronsysteem, maar vanuit een request-portal. Voorbeelden hiervan zijn projectgroepen, gasten, medezeggenschapsraad.
Daarnaast kan ook op basis van bij de aanmelding meegegeven attributen toegang worden verleend. Dit wordt vaak Attribuut Based Access (ABAC) genoemd. De term Situation Based Access is meer op zijn plaats omdat in de andere twee vormen ook sprake is van toegang op basis van attributen.

HAN_

OBAC Rollenmodel HAN

Primair zal de HAN gebruik maken van het Organizational Based Access, op basis van de registraties in de bronsystemen.
Het rollenmodel bepaalt, op basis van de informatie uit de bronregistratie(s) welke toegang een identiteit heeft tot welke omgevingen en informatie. De HAN gebruikt de term 'abonnementen' voor rollen. In een abonnement zitten verschillende rechten gebundeld welke logischerwijze tegelijk worden uitgedeeld.
Uitgaande van de indeling van de verbintenissen geeft het volgende rollenmodel voldoende fijnmazigheid om de rechten binnen de HAN toe te kunnen kennen:

Rol	Rolbasis	Rolinhoud
Basis	Elke HAN-identiteit aangemaakt in het IdM systeem	Account Emailadres Toegang tot intranet Toegang tot portaal
Deelnemer	Elke deelnemer geregistreerd in CATS	Toegang tot ELO Toegang tot Office365
Deelnemer/academie	Alle deelnemers binnen een academie	Toegang tot data-mappen Specifieke toegang tot ELO Toegang tot academie specifieke informatiesystemen
Deelnemer/academie/opleiding	Alle deelnemers aan een specifieke opleiding	Toegang tot opleiding specifieke informatiesystemen
Medewerker	Alle medewerkers geregistreerd in RAET	Toegang tot Office365 Toegang tot centrale data-mappen
Medewerker/academie	Alle medewerkers binnen een academie	Toegang tot academie specifieke data-mappen Toegang tot academie specifieke informatiesystemen
Medewerker/academie/subverbintenis	Alle medewerkers binnen de academie van dit subverbintenis	Toegang tot specifieke informatiesystemen, of informatiesysteemonderdelen.
Medewerker/stafbureau	Alle medewerkers binnen stafbureau	Toegang tot stafbureau specifieke data-mappen
Medewerker/stafbureau/afdeling	Alle medewerkers binnen een afdeling van het stafbureau	Toegang tot afdeling specifieke data-mappen Toegang tot afdeling specifieke informatiesystemen
Overig/subverbintenis	Alle relaties van het betreffende subverbintenis	Toegang tot specifieke informatiesystemen, of informatiesysteemonderdelen.

Let wel: aan één digitale identiteit kunnen meerdere rollen worden gekoppeld. In dergelijke gevallen worden overlappende permissies slechts eenmalig uitgegeven.
Nota bene: naast de automatisch toegekende rollen kunnen altijd rollen op individuele basis worden toegekend.

HAN_

Omgevingen en informatie

Uiteindelijk krijgt een identiteit de beschikking over de informatiesystemen en de data conform de toebedeelde rollen. Deze worden in dit document niet uitgewerkt.

HAN_

User stories

In dit hoofdstuk is een aantal user story's uitgeschreven op basis van de IAM-visie. Ze zijn gegroepeerd op basis van de primaire belanghebbenden. ~~Voor een aantal veelvoorkomende situaties is aangegeven hoe de persoon toegang en rechten verkrijgt (IdM) en deze toegang gebruikt om bij de informatie te komen (AM).~~

Persoon	**MoSCoW**
Als persoon met een nieuwe verbintenis met de HAN wil ik éénmaal mijn gegevens aanvullen zodat ik snel autorisatie verkrijg voor toegang tot gepersonaliseerde informatie.	
Als persoon met een verbintenis wil ik mij maar éénmaal, op één wijze, identificeren zodat ik snel toegang krijg tot alle informatiesystemen waar ik recht op heb (Single SignOn).	
Als persoon met een vroegere verbintenis met de HAN wil ik dat bij een nieuwe verbintenis ik mijn oude identiteitsgegevens kan gebruiken zodat ik geen nieuwe aanmeldprocedures hoef door te lopen.	
Als persoon met een verbintenis met de HAN wil ik op een eenvoudige wijze extra rechten kunnen aanvragen zodat ik snel bij de benodigde informatie(systemen) kan.	
Als persoon met een verbintenis met de HAN wil ik op een eenvoudige wijze mijn identiteitsgegevens kunnen aanpassen zodat ik snel van de nieuwe gegevens gebruik kan maken.	
Als persoon met een verbintenis met de HAN wil ik alleen toegang tot risicovolle informatie(systemen) die ik nodig heb voor mijn activiteiten zodat ik niet per ongeluk gevoelige informatie die niet voor mij bedoeld is kan inzien of verspreiden.	

Student	
Als student van de HAN wil ik over kunnen stappen naar een andere studie zonder mijn identiteit te verliezen zodat ik mijn algemene rechten en middelen niet verlies.	
Medewerker	
Als medewerker studentenadministratie wil ik dat een student automatisch de autorisatie verliest als de studie is afgerond zodat het geen aandacht en tijd kost	
Leidinggevende	
Als leidinggevende wil ik dat mijn nieuwe medewerker direct op de eerste werkdag de autorisaties heeft die nodig zijn voor het werk zodat er geen arbeidsuren verloren gaan aan het regelen van rechten	
Als leidinggevende wil ik tijdig geïnformeerd worden over het verlopen van een inzetcontract zodat ik deze voor afloop kan verlengen.	
Als leidinggevende wil ik dat alle rechten automatisch worden ingetrokken als een medewerker vertrekt zodat ik geen informatieveiligheidsrisico's loop.	
Relatie	
Als relatie van de HAN van een organisatie met een federatieve relatie wil ik met mijn eigen identiteit toegang krijgen tot de informatiesystemen van de HAN zodat ik geen apart HAN account, met alle bijbehorende gegevens, hoeft te hebben.	
Als relatie van de HAN wil ik dat mijn account makkelijk kan worden geactiveerd zodra ik opnieuw werkzaamheden voor de HAN ga uitvoeren.	

HAN_

FG	
Als Functionaris voor de Gegevensbescherming wil ik eenvoudig een auditrapport kunnen opleveren over wie welke rechten heeft zodat ik minder tijd hoef te besteden aan het opleveren van bewijsstukken aan de auditors	
Als Functionaris voor de gegevensbescherming wil ik dat de toegang tot PII altijd beschermd is met een multifactorauthenticatie zodat ik zeker weet dat geen onbevoegden bij PII kan komen.	
Onderzoeksleider	
Als onderzoeksleider wil ik voor een beperkte duur mensen uit de beroepspraktijk toegang geven tot beperkte functionaliteit zodat ik ze eenvoudig bij- en af kan schakelen bij mijn onderzoek.	
Stagebegeleider	
Als stagebegeleider wil ik makkelijk inloggen zodat ik de voortgang van mijn stagiaire kan doorgeven.	
Beheerder	
Als beheerder van de IAM omgeving wil ik dat het IAM systeem de piekbelastingen aan kan zodat deelnemers geen vertraging ervaren bij aanvragen.	
Als beheerder van de IAM omgeving wil ik geen handmatig werk aan nieuwe identiteiten zodat er geen fouten optreden en geen vertraging optreedt	
Als beheerder van de IAM omgeving wil ik eenvoudig organisatieaanpassingen kunnen doorvoeren zodat ik IAM makkelijk kan laten aansluiten bij de flexibele vragen van de organisatie	
Als beheerder van de IAM omgeving wil ik eenvoudig nieuwe informatiesystemen koppelen aan het IAM systeem zodat de toegang snel en efficiënt wordt geregeld	
Bestuurder	
Als Bestuurder wil ik dat alleen relevante informatie, met doelbinding, is opgeslagen in het IAM systeem zodat ik de wet niet overtreedt	
Als Bestuurder wil ik dat voor alle rechten welke worden uitgegeven en ingetrokken vanuit de HAN inzichtelijk is waarom dat gebeurt zodat ik aantoonbaar kan voldoen aan de AVG.	
Als bestuurder van de HAN wil ik dat autorisaties eenvoudig mee veranderen met organisatieaanpassingen zodat de HAN flexibel de veranderingen in organisatie en omgeving kan volgen	
Als bestuurder van de HAN wil ik de verantwoordelijkheden voor het toekennen, intrekken en controleren van autorisaties duidelijk en ‘zo laag mogelijk’ belegd zijn zodat de kans op fouten en datalekken zo klein mogelijk is.	
Informatie Security Officer	
Als Informatie Security Officer wil ik dat de toegang tot informatie afhankelijk is van het risico zodat het aantal informatieveiligheidsincidenten tot een minimum beperkt blijft	
Als Informatie Security Officer wil ik dat de toegang tot kritische informatie altijd beschermd is met een multifactorauthenticatie zodat ik zeker weet dat geen onbevoegden bij kunnen komen.	
Als Informatie Security Officer wil ik dat de mate van toegang die via een federatieve koppeling wordt gegeven afhangt van de mate van vertrouwen (level of Assurance) zodat er geen onveilige verbindingen worden gelegd	

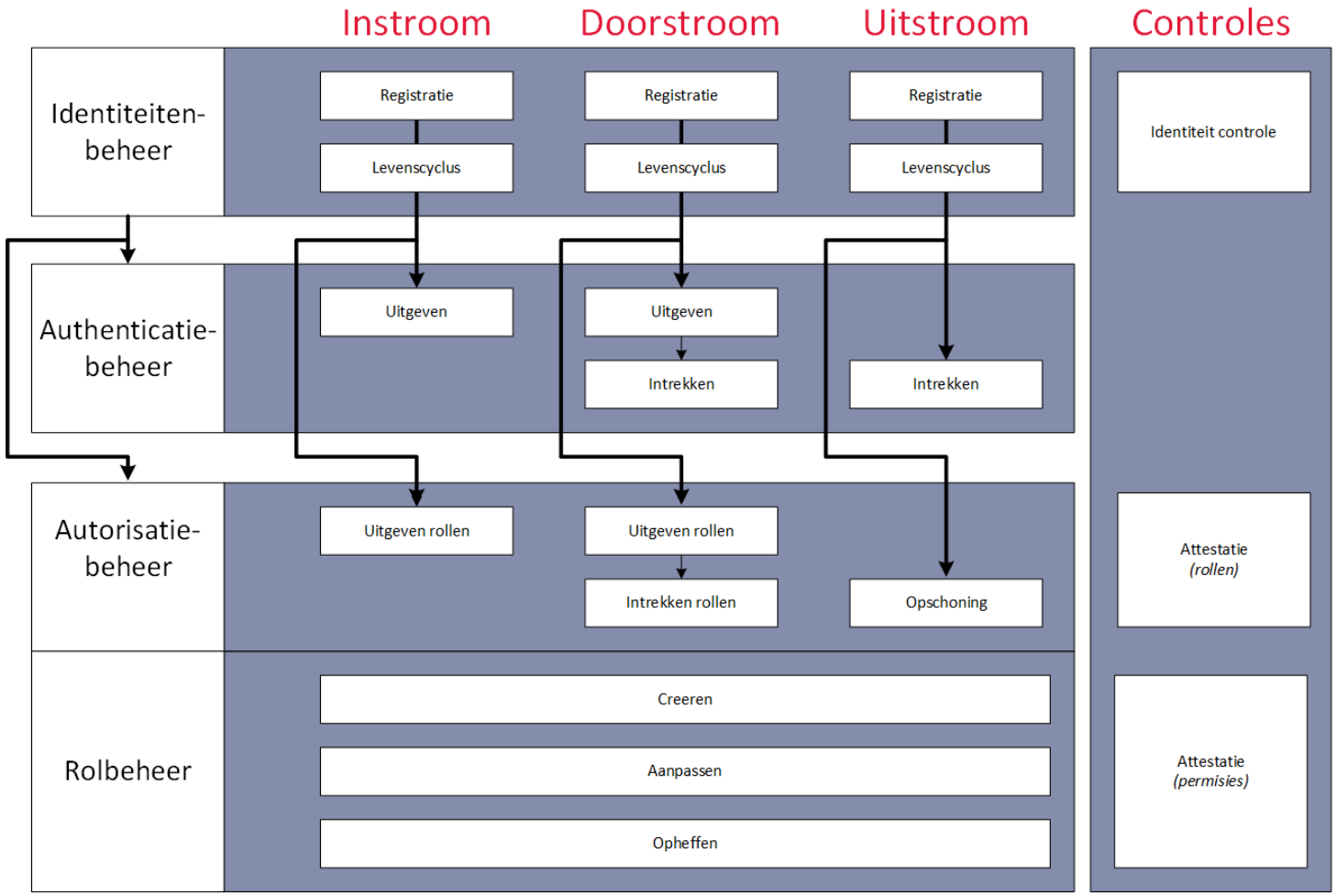
Als Informatie Security Officer wil ik afwijkingen in autorisaties en aanmeldgedrag eenvoudig inzichtelijk is zodat ik tijdig maatregel kan nemen	
Als Informatie Security Officer wil ik inzicht in welke identiteiten veel risico vertegenwoordigen zodat ik passende maatregelen kan nemen	
Als Informatie Security Officer wil ik dat personen die toegang verkrijgen tot kritische informatie zich identificeren met een tweede factor zodat de kans op datalekken verkleind wordt	

Als Informatie Security Officer wil ik dat de accounts van relaties automatisch worden afgesloten als zij niet langer toegang nodig hebben tot de informatiesystemen van de HAN zodat het risico van misbruik en datalekken wordt verlaagd	
Als Informatie Security Officer wil ik dat alle informatie op basis waarvan autorisaties worden toegekend betrouwbaar en volledig zijn zodat niemand de verkeerde autorisaties krijgt	
Enterprise Architect	
Als Enterprise Architect wil ik dat de IAM architectuur onderdeel is van de IT architectuur zodat de impact op IdM van veranderingen in het IT landschap direct inzichtelijk zijn	

IdM processen

In dit schema zijn de subprocessen van IdM weergegeven:
Identiteitenbeheer: het proces van aanmaken, muteren en archiveren van een digitale identiteit; het bewaken van de levenscyclus.
Authenticatiebeheer: het proces rondom het uitgeven en intrekken van authenticatiemiddelen, zoals gebruikersnaam/wachtwoord en multifactorauthenticatiemiddelen
Autorisatiebeheer: het proces rondom het toekennen, muteren en intrekken van rechten
Rolbeheer: het proces rondom het beheren van het rollenmodel.

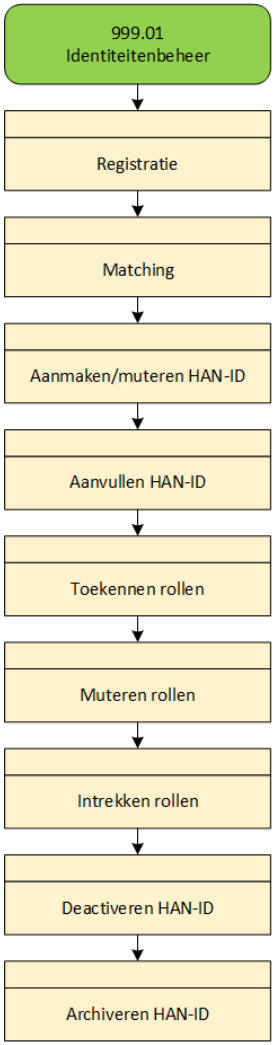
In de laatste kolom staan de mogelijke controles die kunnen worden uitgevoerd om te zorgen dat afwijkingen tijdig worden geconstateerd en gecorrigeerd.



HAN_

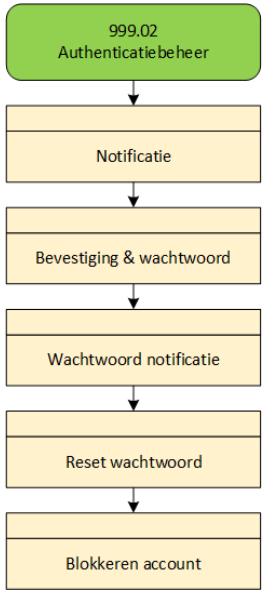
Subprocessen

Identiteitenbeheer



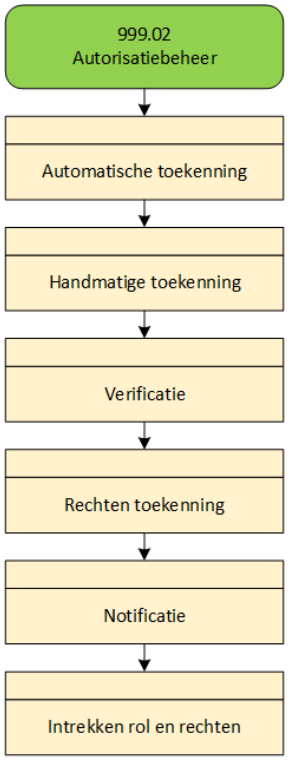
Omschrijving
Persoon wordt geregistreerd in een van de bronsystemen of in het HAN-portal
Nieuwe registratie wordt gematched. Gekeken wordt of de persoon reeds eerder is geregistreerd.
Als de persoon niet bestaat wordt een nieuw HAN-ID aangemaakt. Bestaat de persoon wel al, dan wordt het bijbehorende HAD-ID aangepast.
Via het HAN-portaal kan de persoon de gegevens controleren en ontbrekende gegevens aanvullen
Op basis van de geregistreerde attributen worden de juiste rollen toegekend aan een HAN-ID, inclusief begin- en einddatum en grace-perioden.
Als er gedurende het actieve leven van de HAN-ID zaken veranderen (andere studie/functie/rol) worden de rollen automatisch toegekend of ingetrokken.
Op basis van de einddatum en de 'grace-after' periode worden de rollen ingetrokken.
Op basis van de einddatum en de 'grace-after' periode worden het HAN-ID gedeactiveerd.
Na vastgestelde periode wordt het HAN-ID gearchiveerd en worden er opschoonacties uitgevoerd of uitgezet.

Authenticatiebeheer



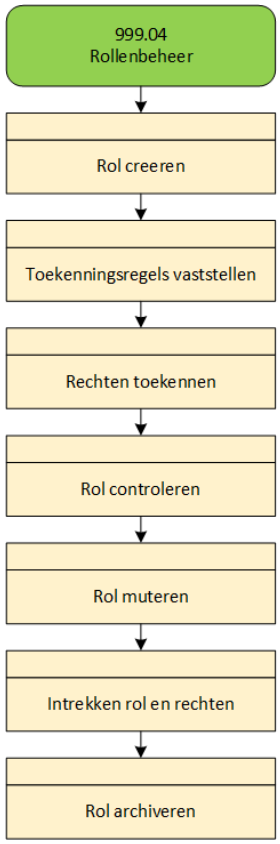
Omschrijving
Een nieuw HAN-ID leidt tot een notificatie naar het privé mailadres
De persoon bevestigt account en zet het wachtwoord
Op basis van wachtwoordregels worden notificaties uitgestuurd als het wachtwoord moet worden aangepast
De persoon past het wachtwoord aan via het HAN-portaal
Op basis van einddatum wordt het account geblokkeerd

Autorisatiebeheer



Omschrijving
Op basis van de attributen van de HAN-ID en het rollenmodel worden een aantal rollen automatisch toegekend aan het HAN-ID
Rollen die niet op basis van de attributen kunnen worden toegekend kunne handmatig door persoon of leidinggevende worden aangevraagd
Indien de rol een verificatie van de roleigenaar vereist wordt deze gevraagd
De rechten welke onder de toegekende rollen behoren worden aan de HAD-ID toegekend
De persoon krijgt een notificatie dat de rechten toegekend zijn. Dit geschiedt uitsluiten in geval van handmatige rollen of rollen met verificatie
Op basis van einddatum van HAN-ID of van de rol worden de rechten onder een beeindigde rol ingetrokken

Rollenbeheer

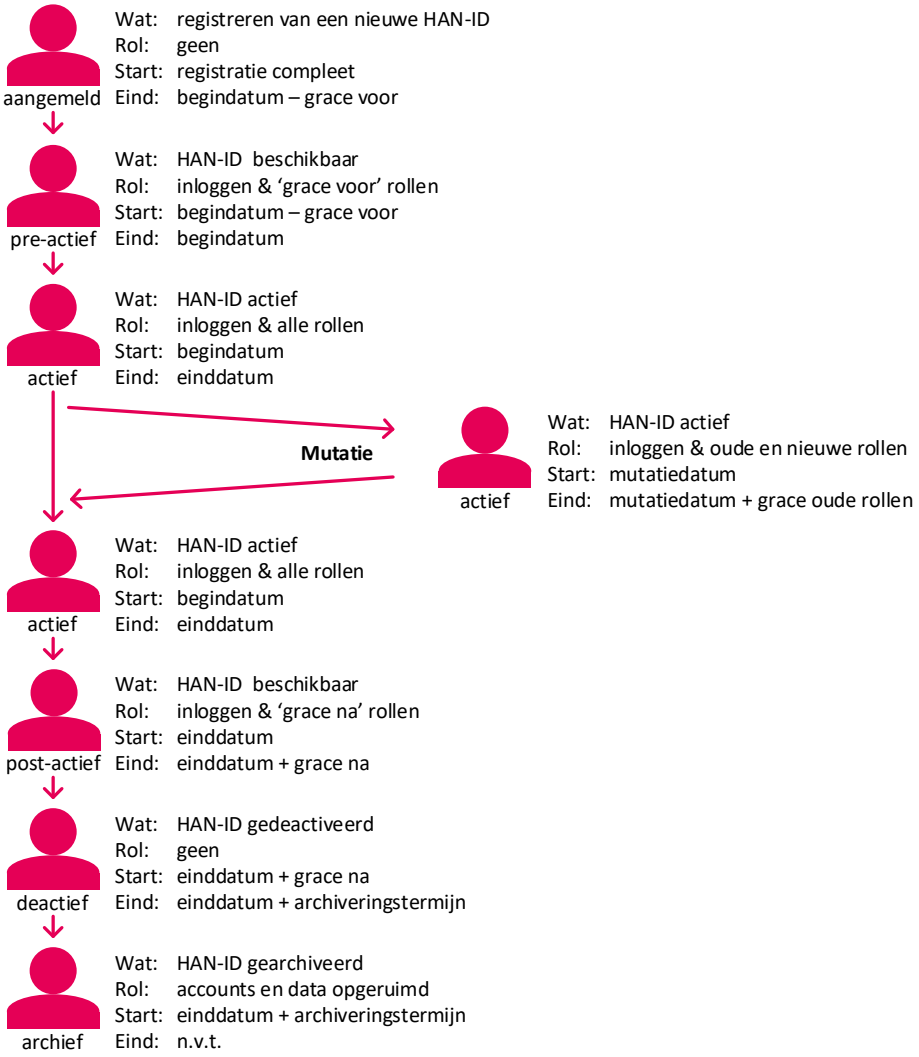


Omschrijving
Op basis van een wijziging in de infrastructuur of organisatie wordt getoetst nieuwe rol aangemaakt
De toekenningsregels worden vastgesteld, en in geval van automatische toekenning in het IdM systeem geborgd.
Aan de rol worden de juiste rechten gekoppeld. Afhankelijk van de configuratie is dat via automatische toekenning of via notificaties
Op regelmatige basis, of voor een grote wijziging, wordt de juistheid van de rol gecontroleerd.
Indien de rol niet juist is worden correcties doorgevoerd. (rechten ingetrokken, toegevoegd, toekenningsregels aangepast)
Als een rol niet langer gebruikt wordt krijgt deze een einddatum. Op die einddatum wordt de rol bij elke HAN-ID waaraan zij is gekoppeld ingetrokken.
Na de einddatum wordt de rol gearchiveerd, zodat die niet langer kan worden toegekend.

Nota bene: De hierboven beschreven subprocessen dienen nog te worden uitgewerkt in gedetailleerde procedures. Hierin wordt vastgelegd welke activiteiten worden uitgevoerd, door wie, waarmee, wanneer en wat het resultaat van elke activiteit is. Dit is onderdeel van het invoeren van een IdM systeem en is mede afhankelijk van de gekozen oplossing en aanpak.

HAN_

HAN-ID Levenscyclus



IdM architectuur

HAN-Portaal

Dit is het portaal waarop eenieder die een HAN-ID heeft zijn eigen gegevens kan aanpassen, zijn wachtwoord kan resetten en rollen kan aanvragen.
Personen die daartoe gerechtigd zijn kunnen via dit portaal ook een HAN-ID of voor een relatie aanvragen, rolaanvragen verifiëren en/of rollen toekennen aan andere HAN-ID's.

Bronsystemen

Dit zijn de systemen waar de basisinformatie omtrent een verbintenis in is vastgelegd.

IDM ID Vault

Dit is de kern van het IdM systeem. Hierin zit alle informatie welke relevant is voor het toekennen en beheren van rechten opgeslagen. De ID Vault is vormgegeven conform het datamodel zoals verderop beschreven

Life Cycle Management

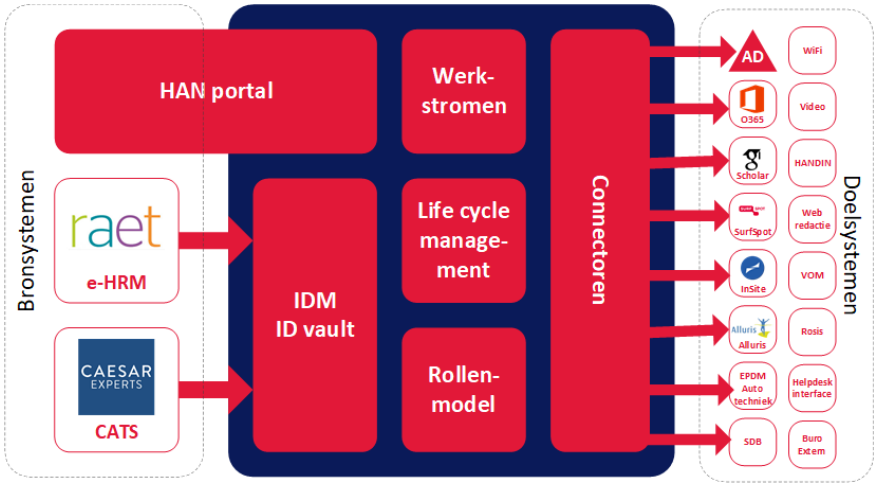
Op basis van de status, begin- en einddata van een HAN-ID en de daaraan gekoppeld rollen zorg het LCM ervoor dat op de juiste momenten de juiste acties door het systeem worden uitgevoerd.

Werkstromen

Indien er menselijk handelen nodig is voor het uitvoeren van een bepaalde actie, bijvoorbeeld verifiëren, van een aanvraag, wordt een werkstroom gestart. Deze notificeert de actor en bewaakt de voortgang van de actie.

Rollenmodel

In het rollenmodel zit de logica opgeslagen op basis waarvan een rol automatisch aan een HAN-ID wordt toegekend. Hierin staan naast de aan de rol koppelde rechten dus ook de toekenningscriteria.



Connectoren

Koppelingen naar doelsystemen, deze zetten de rechten [9] juist in de doelsystemen, op basis van het rollenmodel en signalen uit de werkstromen en het life cycle management.
Afhankelijk van het risico, het volume van aanvragen en de complexiteit van het doelsysteem wordt gebruik gemaakt van een geautomatiseerde koppeling of een notificatie-koppeling[10].

Doelsystemen

De verschillende systemen waar het IDM-systeem de toegang voor de identiteiten voor beheert.

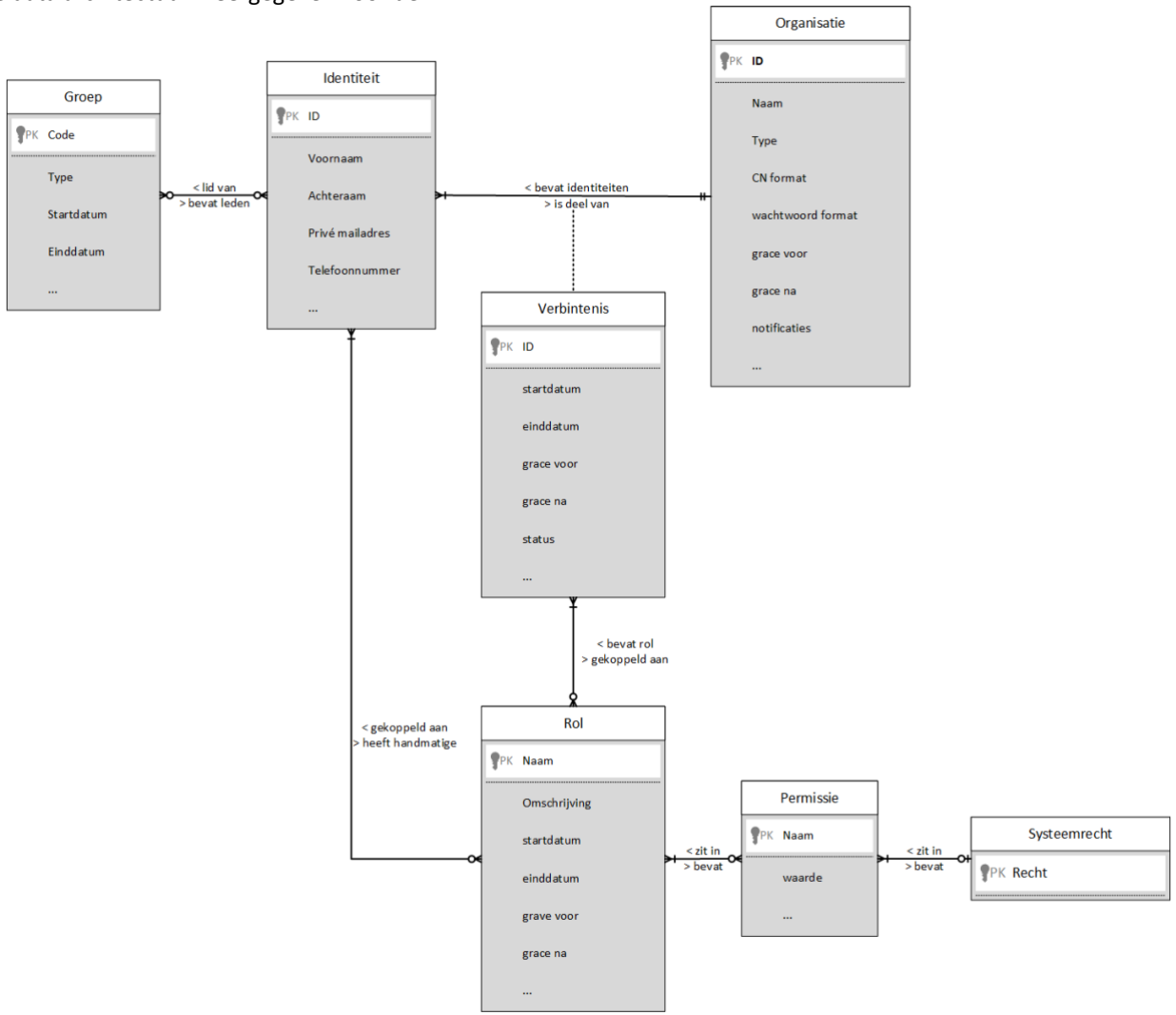
[9] Afhankelijk van de technische mogelijkheden en een kosten/baten afweging kan een connector alleen toegang tot de applicatie regelen of ook rechten in de applicatie.

[10] Een geautomatiseerde koppeling zet rechtstreeks in de applicatie de rechten, een notificatiekoppeling stuurt een bericht met alle benodigde informatie naar de functioneel beheerder met het verzoek de rechten in het systeem aan te passen.

HAN_

Data architectuur

In onderstaand schema is de data architectuur weergegeven voor de HAN.

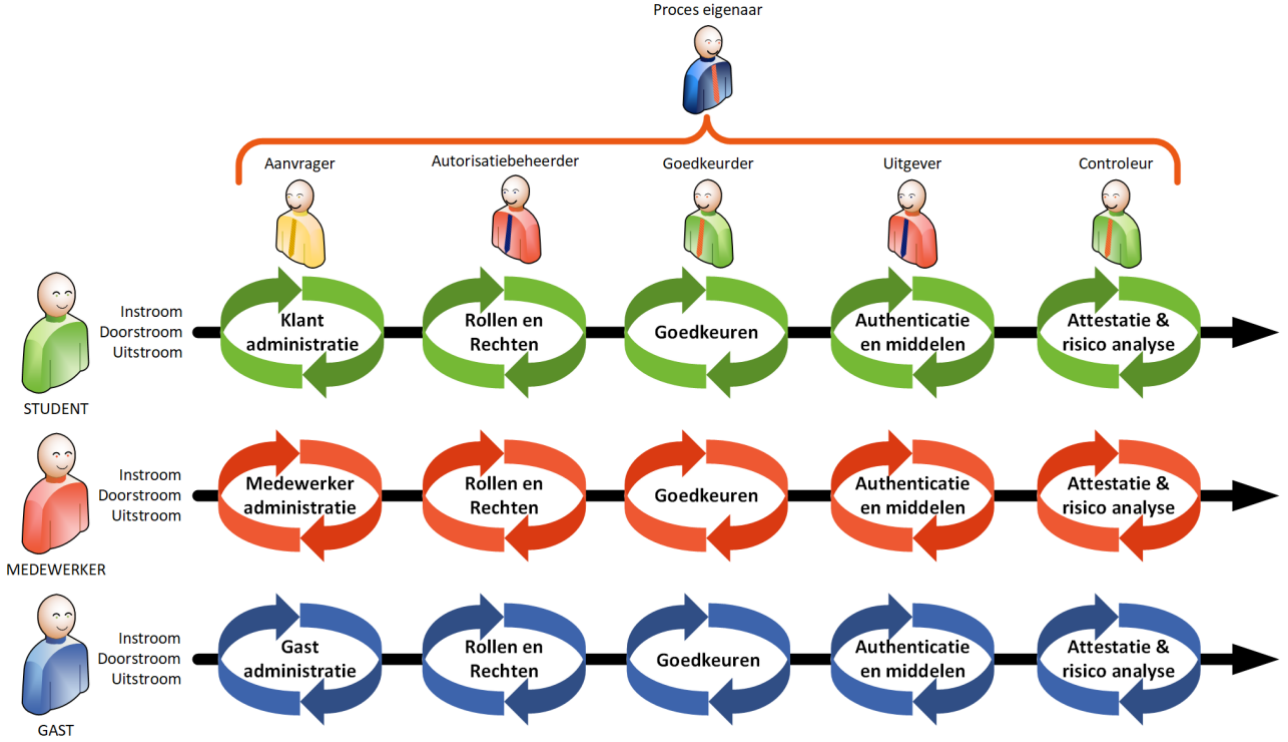


Entiteit	Omschrijving	Relaties	Voorbeelden
Groep	Een collectie gebruikers welke handmatig of op basis van regels gegroepeerd worden om rechten te delen of voor synchronisatie naar een doelsysteem.	Identiteit	Klasgroep Cohortgroep Projectgroep
Identiteit	De uniek digitale representatie van een natuurlijk persoon binnen de HAN.	Groep Organisatie (via verbintenis) Handmatig toekenede rol	Persoon
Organisatie	Een (deel)organisatie waar een eigen configuratie aan gekoppeld kan worden. Iedere IDM-systeem heeft ten minste één organisatie.	Identiteit (via verbintenis)	HAN
Verbintenis	Een relatie tussen de identiteit en zijn organisatie.	Identiteit Organisatie Rol	Medewerker Deelnemer Overig
Rol	Een logische bundeling van rechten welke altijd gelijktijdig wordt toegekend en ingetrokken.	Identiteit (indien handmatig toegekend) Verbintenis (indien automatisch toegekend	DeelnemerGezondheid MedewerkerPersonnelszaken OverigeStagebegeleiderTechniekenLifeScienes
Permissie	Een specifiek recht tot een specifieke vorm van toegang	Rol	XeduleRoosterplannen HAN-QMPDeelnemenToetsen
Systeemrecht	Het specifieke recht op het doelsysteem	Permissie	Xedule/…/.../…/… HAN-QMP/…/…/…

IAM organisatie

Organisatorische verantwoordelijkheden.

Het functioneel beheer van IAM gebeurt door de HAN zelf. De verschillende organisatorische taken die daarbinnen te definiëren zijn worden hieronder schematisch weergegeven in relatie met de verschillende processen welke gedurende de levensloop van een identiteit optreden. Het is goed mogelijk dat taken voor een bepaalde set aan rollen gebundeld zijn. Zo liggen de taak van goedkeurder en de taak van controleur vaak bij een de dezelfde persoon. Hetzelfde geldt voor de autorisatiebeheerder en uitgevertaak, die vaak bij een functioneel beheerder van een informatiesysteem liggen.



Waar we in dit plaatje spreken van ‘rollen en rechten’ worden rollen of attributen bedoeld, zoals beschreven in bijlage II van het visie document. Deze rollen worden gebruikt bij (basis) Identity Management en bij federatie binnen Access Management. Zie hiervoor het visie document: het hoofdstuk ‘Overzicht over IAM-functies.’ Het goedkeuren is bij rollen die automatisch worden toegekend (door provisioning of via federatie) eenmalig totdat daarin een wijziging optreedt, maar het kan ook gaan om ad hoc goedkeuren bij het aanvragen van rollen door gebruikers.

HAN_

Proceseigenaar

De proceseigenaar is verantwoordelijk voor het volledige IdM-proces.

Taak	– Overziet het IdM-landschap binnen de organisatie – Kan beslissingen nemen of besluiten verkrijgen – Weet wie wat weet binnen de organisatie en kan deze aanspreken – Zorgt voor afstemming met andere beleidsgebieden als personeelszaken, informatieveiligheid, privacy, compliance, financiën en onderwijs en onderzoek – Bewaakt de processen – Bewaakt het rollenmodel – Bewaakt de regels voor het toekennen van rollen en rechten – Waakt ervoor dat de IdM-doelen aansluiten bij de HAN-doelstellingen en worden behaald
Belegging	Deze rol kan belegd worden bij een functionaris met voldoende mandaat. De rol kan ook opgesplitst worden, bijvoorbeeld in een overall verantwoordelijkheid en een verantwoordelijkheid voor processen en coördinatie van het rollenmodel.

Aanvrager

De aanvrager zorgt ervoor dat de juiste rollen worden aangevraagd, dit is uitsluitend van belang voor additionele taakrollen en voor extra attributen voor federatieve koppelingen.

Taak	– Vraagt op functioneel niveau additionele rollen aan voor in- en doorstroom via het manager-portaal
Belegging	Zo dicht mogelijk bij de uitvoering: docent, manager

Autorisatiebeheerder

De autorisatiebeheerder zorgt ervoor dat de rollen de juiste inhoud hebben.

Taak	– Vertaalt de functionele rollen naar technische rechten en beheert de rollen binnen een domein. – Voegt toekenningsregels toe aan basis en automatische rollen en beheert deze – Zorgt voor juiste functionele beschrijvingen van de rollen zodat aanvragers ze begrijpen – Is – waar nodig - intermediair tussen goedkeurder en informatiesysteembeheerders – Kan op vraag inzicht geven in inhoud, gebruik en reden van een rol.
Belegging	Dichtbij of onderdeel van de lijnorganisatie met affiniteit voor IT: docent, manager Wel functioneel centraal aangestuurd door de proceseigenaar om synergievoordelen te behalen

Goedkeurder

De goedkeurder geeft de formele goedkeuring voor toekennen van risicovolle rollen. Dit kunnen rollen zijn die door een gebruiker of door een manager voor een gebruikers zijn aangevraagd.

Taak	– Akkoord geven op het uitgeven van risicovolle rollen.
	Risico kan zijn:
	  – toegang tot persoonsinformatie (in kader van AVG)
	  – toegang tot bedrijfskritische of mediagevoelige informatie
	  – toegang tot intellectueel eigendom
	  – gebruik van kostbare licenties
	  – schenden van functiescheidingsregels
	– Dit akkoord betreft zowel akkoord op de toekenningsregels van basis- en automatische rollen als ad hoc voor additionele rollen.

Belegging	Voor elke risico-rol wordt een goedkeurder vastgesteld, welke afhankelijk van het type risico kan liggen bij een manager, de eigenaar van de informatie(systemen) of control (security/compliance/risk).

Uitgever

Een uitgever zorgt dat de benodigde rechten of middelen worden uitgegeven, en weer worden ingenomen. Afhankelijk van de soort koppeling is de uitgever verantwoordelijk voor het juist werken van de automatische koppeling tussen het IAM-systeem en het doel systeem of het uitvoeren van handmatige taken in het doelsysteem op basis van notificaties uit het IAM-systeem.

Taak	– Op aangeven van notificaties vanuit IdM systeem (TOPdesk tickets) uitgeven of intrekken van rechten in doelsystemen of uitgeven of innemen van fysieke middelen. – Zorgen dat de juiste informatie wordt ontvangen van het IdM-systeem
Belegging	Bij de beheerders van de rechten / middelen

Controleur

De controleur controleert op regelmatige basis de uitgegeven rechten, met name de toegestane uitzonderingen.

Taak	– Verifieert de uitgegeven rechten en zorgt dat er acties worden genomen als er fouten worden aangetroffen. – Uitvoeren van attestatie controles: kloppen de toekenningsregels en additioneel uitgegeven rollen nog steeds.
Belegging	Hangt af van het risico en de formele verplichtingen. Vaak bij dezelfde persoon als de goedkeurder. Daarnaast in- en externe auditors

HAN_

IAM-oplossingen

In lijn met het hoofdstuk 'IDaaS en PaaS opties' uit het visiedocument en het feit dat onderhoud van IAM-systemen complex is en specifieke kennis vraagt[11], ligt het voor de hand geen on-premise oplossingen in eigen beheer te gebruiken.

Het volgende is dan het advies:

- Gebruik voor basis IAM-functies een PaaS-oplossing of een door een leverancier beheerde on-premise oplossing. IDaaS-oplossingen zijn op dit moment alleen geschikt om zeer goed gestandaardiseerde cloud-applicaties te voorzien van gebruikersaccounts en rechten. Een hybride-oplossing (IDaaS/PaaS of IDaaS/on-premise) is ook een optie.
- Gebruik voor Access Management een IDaaS-oplossing. Deze zijn momenteel volwassen en uitgebreid genoeg om de use cases van de HAN voldoende veilig in te vullen. Het kunnen overigens ook gecombineerde diensten zijn (MFA van de ene leverancier, federatie van een andere, etc.). De leveranciers kunnen dat prima aan.
- Gebruik voor Identity governance een IDaaS-oplossing of PaaS-oplossing. Deze zijn momenteel volwassen en uitgebreid genoeg om de use cases van de HAN voldoende veilig in te vullen.

[11] Zie ook de inleiding van het visiedocument.