Identity & Acces Management bij Kentalis

Datum	20-11-2023
Versie	1
Status	goedgekeurd
Auteur	Edwin van der Heijden
E	Ed.vanderHeijden@kentalis.nl

Koninklijke Kentalis

Inhoud

Inhoud

Documentgegevens

Versiebeheer

Versie	Datum	Auteur	Samenvatting van de wijzigingen	Jira
0.1	13-11-2023	Edwin van der Heijden	Eerste versie	IAM-348
0.2	20-11-2023	Edwin van der Heijden	Review van Steven verwerkt	IAM-348
1.0	23-11-2023	Edwin van der Heijden	Goedkeuring IAM team	IAM-348

Gerelateerde documenten

Documentnaam	Beschrijving	Vindplaats document
IAM-SA	Solution architectuur	Projectmap / 60. Architectuur
Richtlijnen IAM	IAM binnen Kentalis	Teams IAM
Solution Architectuur Identity & Access Management Kentalis v1.1	Bevat o.a. de scope van RBAC	Teams IAM

1 INLEIDING

1.1 AANLEIDING

Kentalis beheert en onderhoud identiteiten, de daaraan gekoppelde gegevens en de toegang die deze identiteiten zijn momenteel decentraal. Het beheer gaat echter meer gecentraliseerd worden en centraal aangestuurd in een multidisciplinair team (IAM). Daarmee wordt ook het huidige proces herzien en waar mogelijke geautomatiseerd. De gevolgen van deze beslissing raakt alle onderdelen van de organisatie en vergt een (verregaande) aanpassing van denkwijzen en applicatie inrichting.

1.2 DOELSTELLING

Dit document is een globaal procesdocument over de taken en verantwoordelijkheden van het Team IAM (Identity & Access Management) en kan beschouwd worden als kennismaken met IAM bij Kentalis.

Omdat de term IAM niet overeenkomt met de werkelijke invulling van de werkzaamheden is het beter de term IGA te gebruiken. IGA staat voor Identity Governance & Administration en stelt organisaties in staat digitale identiteiten en IT-resources binnen de organisatie te beheren. IGA gaat dan zowel over de uitvoering en beveiliging als over het beleid. IGA is een term die internationaal in gebruik is en langzamerhand de term IAM doet vervangen. In communicatie van onze afdeling zal je deze term dan ook terugvinden.

1.3 DOELGROEP

De doelgroepen van dit document zijn de informatiemanagers, functioneel beheerders, eigenaren van bron- en doelsystemen, decentrale beheerders, en de (interne) auditors.

2 DOEL VAN IDENTITY EN ACCES MANGEMENT

Met de invoering IAM worden verschillende doelen bereikt. Elk van deze doelen heeft als belangrijkste kenmerk dat we het veiliger en makkelijker willen maken voor onze gebruikers. Verder in het document wordt uitleg gegeven hoe de inrichting van een goed IGA-proces daaraan kan bijdragen. Het belang van elk van deze doelen kan verschillend gewogen worden, al naar gelang bedrijfsdoelstellingen.

Vergroten gebruikersgemak

Het IGA-proces verbetert de beheersbaarheid van het aanvragen en toekennen van autorisaties. Door vooraf gedefinieerde rollen worden bepaalde autorisaties standaard doorgevoerd op basis van de positie of aanstelling van een medewerker. Gebruikers worden zodoende bij indiensttreding automatisch voorzien van de juiste rechten, waardoor onoverzichtelijke en tijdrovende aanvragen tot het verleden gaan behoren.
Daarnaast worden serviceaanvragen met ‘losse autorisatie-verzoeken’ overzichtelijker door gebruik van deze rolstructuur. Geautoriseerde aanvragers worden voorzien van een portaal waar ze ad-hoc aanvragen rechtstreeks kunnen invoeren waarna deze (indien gewenst) direct beschikbaar zijn. Medewerkers beschikken sneller over de juiste autorisaties en daarmee toegang tot informatie.

Verbeteren van transparantie

Door het IGA-proces compleet in te richten wordt er vanuit het oogpunt van de bedrijfsprocessen voor gezorgd dat, de gebruikers van onze systemen alleen tot die informatie en systemen toegang hebben die nodig zijn voor hun werk of studie. Hiermee kan worden aangetoond dat we werken aan het ‘in control en compliant’ zijn ten aanzien van geldende wet- en regelgeving, zoals de Wet Bescherming Persoonsgegevens, en interne regels.

Verbeteren van het niveau van informatiebeveiliging:

Doordat autorisaties worden geclusterd en gekoppeld aan een rol, is altijd duidelijk wat een rol mag of kan. Doordat de gebruikers van onze systemen worden gekoppeld aan rollen, is daarmee altijd inzichtelijk wie toegang heeft tot welke informatie. Door deze clustering (meerdere personen kunnen eenzelfde rol hebben) is het aantal autorisaties lager waarmee de kans op fouten afneemt. Door centraal vast te stellen wie rollen kan aanmaken of beheren, is het geheel van informatiebeveiliging beter in beeld.

Verbeteren van controleerbaarheid

IAM kan ‘monitoring en audit’-mogelijkheden bieden voor interne, externe en ad-hoc rapportages. Uiteindelijk biedt dit IGA-proces de mogelijkheid om aantoonbaar ‘in control’ te zijn ten aanzien van wie waartoe toegang heeft.

Verbeteren van de beheersbaarheid

Door IAM zowel technisch als functioneel (procesmatig) verder te standaardiseren, kunnen ook procedures, binnen de organisatieonderdelen, voor het aanvragen en toekennen van autorisaties worden gestandaardiseerd, verminderd en/of worden ingericht.

Kostenbeheersing

Het IGA-proces maakt het mogelijk om eenvoudig te bepalen wie toegang moet hebben tot welk materiaal. Door dit middel in te zetten, bestaat de mogelijkheid kosten te besparen op bijvoorbeeld softwarelicenties.

Verbeteren van functiescheiding

Door het IGA-proces kan centraal en in overeenstemming met beleid functiescheiding beter worden gerealiseerd en inzichtelijk gemaakt. Tijdens het beschrijven en inrichten van de rollen en achteraf bij audits, kan bepaald worden welke rollen niet in één functie verenigd mogen worden.

3 MODEL IDENTITY EN ACCES MANAGMENT

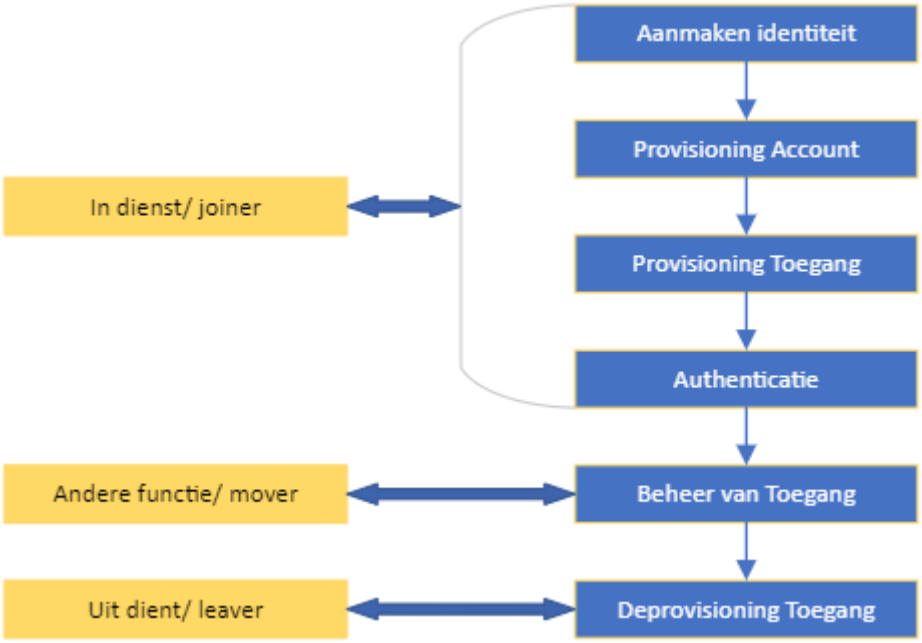
IAM is de verbindende schakel tussen onze business- en IT-organisatie. Het verbindt organisatiekenmerken, zoals het organogram, functies en taken aan IT-diensten.

Zoals eerder aangegeven is de term IAM daarom eigenlijk een verouderde term, intussen ingehaald door vernieuwde inzichten. Identity en Acces Management kan namelijk niet los gezien worden van de bedrijfsprocessen en beleidsbepalingen.

Aangezien Kentalis de naamgeving IAM heeft gekozen voor de afdeling zal deze term voor de afdeling blijven gelden, echter het achterliggende model zal het IGA model genoemd worden.

3.1 WERKZAAMHEDEN IAM

Kort samengevat is het team IAM verantwoordelijk voor het aanmaken, beheren, controleren en intrekken van uitgegeven (digitale) identiteiten.



Afdeelding 1

Eén natuurlijk geïdentificeerd persoon krijgt één digitale identiteit binnen één van onze bronsystemen. Aan de hand van de kenmerken van het bronsysteem geeft kan deze persoon de identiteit gebruiken voor authenticatie in onze systemen. Het kan dus zijn dat één natuurlijk persoon binnen meerdere bronsystemen bestaat, deze heeft dan een andere kenmerken en een andere login.
In onderstaande tabel staan de verschillende typen identiteiten weergegeven welke voorkomen bij Kentalis. Types verschillen van elkaar in de manier van administreren, de levensloop, en/of de gebruikte of gegenereerde attributen.

Type	Subtype	Bronsysteem
Medewerker	Medewerker Stagiaire ZZP-er Uitzendkracht Vakantiekracht Externe medewerker	AFAS (zorg) AFAS (onderwijs)[1]
Leerling	Leerling	ParnasSys
Cliënt[2]	Cliënt	USER
Leverancier[3]	Leveranciers	Leveranciersadministratie
Toezichthouder[4]	Toezichthouders	N.t.b.
Verzorgers[4]	Ouder, voogd, et cetera	N.t.b.

Afdeelding 2

[1] In AFAS zijn twee gescheiden omgevingen gecreëerd voor zorg- en onderwijspersoneel. Persoren die een aanstelling in beide omgevingen hebben worden door het IGA-systeem gezien als twee gescheiden identiteiten.

[2] USER is nog niet als bornsysteem aan IGA gekoppeld. Identiteiten voor Cliënten worden niet door IGA beheerd.

[3] De leveranciersadministratie is ingericht maar nog niet in productie genomen

[4] Er is nog geen administratie ingericht voor overige derden (toezichthouders, verzorgers, etc.)

De beschrijving van deze identiteiten is opgenomen in het document: “solution architectuur identity & acces management”, zie gerelateerde documenten.

3.2 ROLLEN EN PERMISSIES

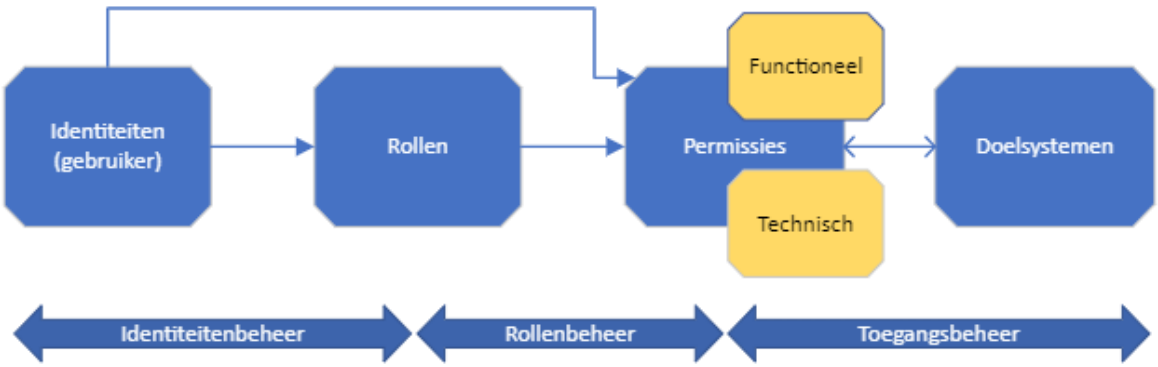
Om uit te leggen hoe het IGA-model tot stand komt is het belangrijk om eerste de begrippen Rol en Permissie uit te leggen en de samenhang daartussen.
Het concept is in principe simpel, een rol is abstractie van de relatie tussen een identiteit (gebruiker) en een permissie. Een identiteit kan meerdere rollen bevatten en een rol kan meerdere permissies bevatten.

Afbeelding 3

In hiërarchische volgorde kan een rol worden toegekend aan een andere rol. Een rol heeft daarnaast nog enkele andere kenmerken. Zo kan een rol restricties hebben en niet aan andere specifieke rollen gekoppeld worden, zogenoemde functiescheiding. Ook kan een rol tijdsgebonden of plaatsgebonden kenmerken bevatten (denk aan tijdelijke toegang voor een gastdocent op een bepaalde school).

Het beheer van dit IGA-model wordt ingedeeld in drie hoofdtaken. Deze taken worden niet allemaal door de afdeling IAM vervuld maar hebben wel direct een raakvlak met het IGA proces. Deze taken kunnen derhalve ook belegd zijn binnen meerdere bedrijfsfuncties.

- Identiteitenbeheer: Zorgt voor het creëren van een digitale identiteit op basis van een vastlegging van persoonsgegevens in een bronsysteem.
- Rollenbeheer: Zorgt voor het toekennen van de juiste permissies (rechten in doelsystemen) aan digitale identiteiten op basis van attributen uit een bronsysteem of op basis van geautoriseerde aanvragen, vastgelegd in rollen.
- Toegangsbeheer: Zorgt het juiste niveau van beveiliging van de toegang tot de informatiesystemen van Kentalis



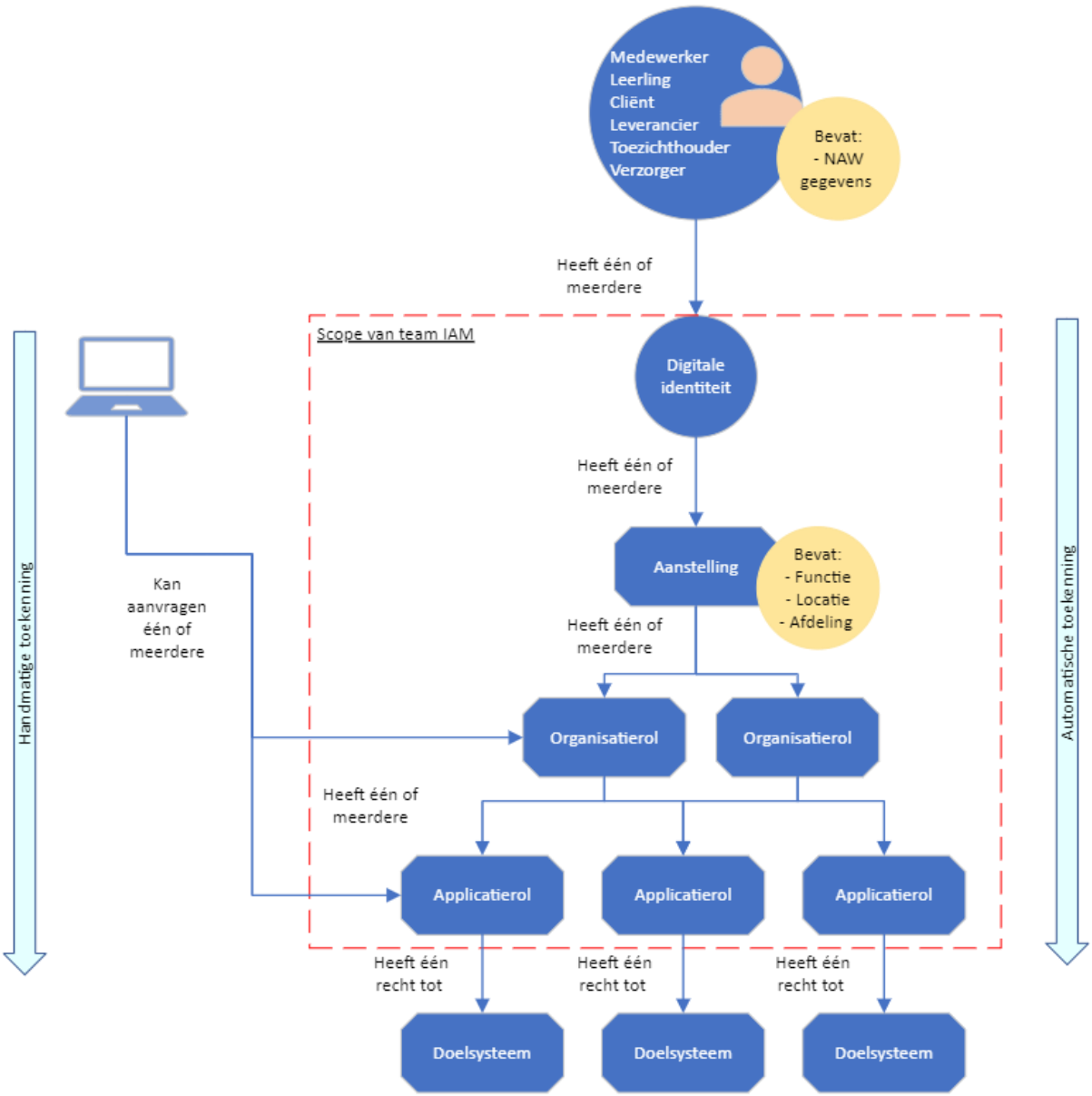
Taken:

- *Identiteitenbeheer*: Het aanmaken, muteren, bewaken van de levensloop en archiveren van digitale identiteiten op basis van registratie van natuurlijke personen en niet persoonlijke entiteiten in de bronsystemen.
- *Rollenbeheer:* Het toekennen en intrekken van rechten aan digitale identiteiten die het gebruik van applicaties waarvoor Kentalis verwerkingsverantwoordelijkheid heeft reguleert.
- *Toegangsbeheer:* Het voorzien van een authenticatiemethode voor toegang tot informatiesystemen. Hier valt ook het beheer van individuele koppelingen tussen identiteiten en functionele autorisaties onder (dus zonder tussenkomst van een rol, denk aan een financieel directeur die een medewerker expliciet autorisatie geeft om betalingen te verrichten). Vaak ingericht door de applicatiebeheerder.

3.2 ROLMODEL

In het rolmodel staat beschreven welke rollen een (type)identiteit toegekend krijgt en hoe deze aangevraagd kunnen worden.

Onderstaand is globaal weergegeven het Kentalis rolmodel.



- Organisatierol: Op basis van de aanstelling in het bronsysteem worden automatische een basisrol toegekend aan de identiteit.
- Applicatierol: Op basis van de functie wordt aan een medewerker automatisch één of meerdere bedrijfsrollen toegekend. Dit kan zijn op basis van de organisatorische plek binnen de organisatie of waar iemand werkt of studeert. Daarnaast kunnen extra rollen door een daartoe bevoegd persoon worden aangevraagd*.
- Handmatige toekenning: Op basis van specifieke wensen, nevenactiviteiten of organisatorische wensen kan één rol handmatig aangevraagd en toegekend worden*.

  * Deze aanvraag gaat nu via de service management tool, deze zal waar mogelijk vervangen worden door een automatische oplossing zodat aanpassingen per direct zichtbaar zijn. Uiteraard met voorwaarden die door team IAM beheerd worden.

3.3 RBAC (ROLE BASED ACCESS)

Nu we een globaal rolmodel hebben is het natuurlijk belangrijk om de inrichting van die rollen zo te definiëren dat identiteiten ook alleen toegang hebben tot de systemen en data die ze daadwerkelijk mogen inzien.

Gegevensbeheer van identiteiten voor medewerkers, leerlingen en gasten is belegd en ingericht in onze bronsystemen. Deze systemen zijn gekoppeld met het IGA-systeem die deze gegevens verrijkt en voorziet van de juiste identiteitsgegevens voor de digitale identiteit.
Aan deze digitale identiteit wordt de functie gekoppeld welke in de bronsystemen zijn opgenomen.
RBAC is het concept waarop het rolmodel is ingericht en beschrijft dat identiteiten niet rechtstreeks worden geautoriseerd in informatiesystemen, maar dat ze uitsluitend rechten krijgen door een vorm van groepslidmaatschap, op basis van de rol die ze hebben binnen een organisatie of bedrijfsproces.

RBAC geeft handvaten om de koppeling en groepering van de permissies op objecten/functies in informatiesystemen in te richten. Denk bijvoorbeeld aan de criteria die een functie kan bevatten zoals locatie en afdeling die van invloed kan zijn op de permissies die je krijgt.

Door het koppelen van de rol van de gebruiker in de organisatie aan een rol in een informatiesysteem, is het eenvoudig om de effectieve rechten van een gebruiker te bepalen. Het daadwerkelijk toekennen van rechten en permissies aan een gebruiker en het verstrekken van gerelateerde objecten (tokens en dergelijke) heet provisioning. Provisioning van onze systemen gebeurd real time, wat wil zeggen dat aanpassingen direct zichtbaar zijn.

Het uitgeschreven RBAC proces is terug te vinden in de tooling “Bookstack”. Indien gewenst kan dit worden ingezien door een aanvraag te doen bij het team IAM.
Opm. Het is in de nabije toekomst wenselijk om dit voor de doelgroep beschikbaar te maken.

3.3 ROLBEHEER

Eigenaarschap en (functioneel) beheer zijn noodzakelijke voorwaarden voor identity management. Voor de juiste uitvoering zal het volgend bekend moeten zijn:

- Wie is de eigenaar van de applicatie (dienst) en dus eigenaar dan de applicatierollen?
- Wie is de eigenaar van bedrijfsrollen?
- Wie is verantwoordelijk voor rollenbeheer?
- Wie is verantwoordelijk voor een goede toepassing van functiescheiding?

Deze zaken zijn vastgelegd, gecommuniceerd met betrokkenen en worden nageleefd.

Alle informatie over (bedrijfs)rollen en functiescheidingen is terug te vinden in de tooling “Bookstack”. Indien gewenst kan dit worden ingezien door een aanvraag te doen bij het team IAM.

Opm. Het is in de nabije toekomst wenselijk om dit voor de doelgroep beschikbaar te maken.

Applicatie eigenaren worden vastgesteld door Informatiemanagement.

4 BEGRIPPENLIJST

Applicatierol	Een logische bundeling van systeemrechten in een doelsysteem, binnen het IGA-systeem gerepresenteerd als een permissie.
Bronsysteem	Een applicatie of IT-platform welke als betrouwbare bron wordt gebruikt voor het leveren van gegevens over personen of niet persoonlijke subjecten. Voor beide zijn het bronsysteem leidend, hetgeen wil zeggen dat het bepaalt of een identiteit aanwezig mag zijn of niet.Het is mogelijk dat er verschillende bronsystemen zijn voor één identiteit, maar alleen als leverancier van andere gegevens.
Digitale identiteit	Een digitale representatie van een natuurlijk persoon met unieke identificerende referenties en kenmerken, op basis waarvan toegang kan worden verleend tot een *IT-dienst*.
Doelsysteem	Een applicatie of IT-platform waarvoor de autorisaties worden beheerd in het IGA-systeem.
IAM	Identity & Access Management, andere term voor Identity Governance & Administration (IGA).
IGA	Identity Governance & Administration, het geheel aan processen, systemen en organisatie om ervoor te zorgen dat de juiste subjecten, voor de juiste redenen en op het juiste moment toegang krijgen tot de juiste IT-diensten.
IGA-proces	Identity Governance & Administration, het geheel aan processen, systemen en organisatie om ervoor te zorgen dat de juiste subjecten, voor de juiste redenen en op het juiste moment toegang krijgen tot de juiste IT-diensten.
IGA-systeem	Geautomatiseerd hulpmiddel dat de processen voor uitgeven en intrekken van rechten ondersteunt.
IT-dienst	Een applicatie, IT-platform, IT-service, functionaliteit of gegevens, waar subject toegang toe moet hebben om een actie uit te kunnen voeren.
Natuurlijk persoon	Een natuurlijk persoon is een mens in juridische zin, als iemand die drager van rechten en verplichtingen kan zijn.
Organisatie	Kentalis
Organisatierol	Een rol gedefinieerd door de organisatieplaats van de identiteit, zoals afdeling, functie en/of locatie.
permissie	De weergave in een IGA-systeem van een autorisatie in een doelsysteem. Over het algemeen een-op-een gekoppeld aan dat recht

Persoon	Een natuurlijk persoon dat een aanstelling heeft met Kentalis.
Provisioning	De technologie die ervoor zorgt dat digitale identiteiten automatisch worden aangemaakt, gewijzigd, uitgeschakeld en verwijderd.
Rol	Een rol is abstractie van de relatie tussen een identiteit (gebruiker) en een permissie.
Rolmodel	Model waarin de logica achter het toekennen en intrekken van rechten is vastgelegd, gebruikmakend van rollen.
Validatie	Een bevestiging dat iets voldoet aan een overeengekomen specificatie.