T 030 275 33 30
www.kentalis.nl
KvK 02070578

Van Vollenhovenlaan 659-661
3527 JP Utrecht
Postbus 89
3500 AB Utrecht

IAM Aansluitvoorwaarden Doelsystemen

Zodat Kentalis gebruikers en rechten kan provisionen

Datum	2-6-2025
Kenmerk	
Versie	3.1
Status	Definitief
Auteurs	Roel van der Zanden, Robert Wielinga, Steven van der Linden, Nick Heuvelink, Maurits van Boetzelaer

Inhoud

Documentgegevens

Versiebeheer

Versie	Datum	Auteur	Samenvatting van de wijzigingen	JIRA
0.1	2-11-2022	M.W.J. van Boetzelaer	Eerste opzet	IAM-206
2.1	28-8-2023	S.F. van der Linden	Verplaatst en bijgewerkt	IAM-401
2.2	27-2-2024	R. Wielinga	Bijgewerkt	IAM-494
3.0	3-1-2024	R. Wielinga	Bijgewerkt	IAM-554
3.1	2-6-2025	R. van der Zanden / S. van der Linden	Provisioning (H3) aangepast	

Distributie

Naam	Functie	Rol	v0.1	v0.2	v0.9	v1.0

Goedkeuring

Rol	Naam	Datum	Vrijgave/Akkoord
Product Owner	M. Gresnigt		

Gerelateerde documenten

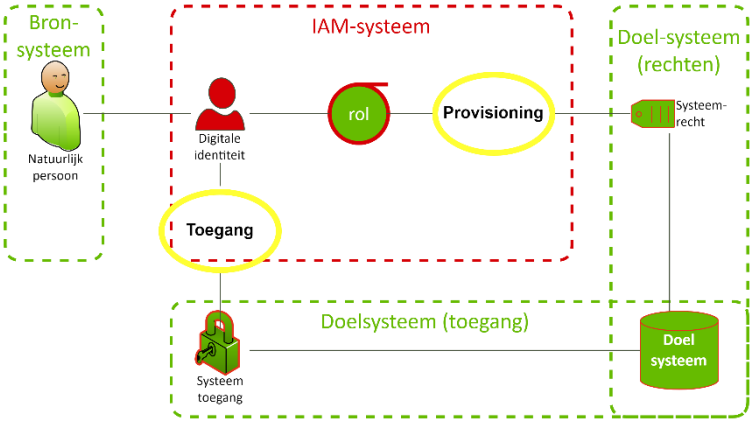
Documentnaam	Beschrijving	Vindplaats document
Solution Architectuur Identity & Access Management Kentalis	Architectuur	SA IAM

1 Inleiding

Kentalis wil controle houden op het gebruik van identiteitsgegevens en autorisaties van haar medewerkers in haar systemen, zodat het voldoet aan de hiervoor gespecificeerde eisen in de NEN7510. Deze controle wordt geborgd door het gebruik van een Identity en Access Management (IAM) systeem. Dit systeem betrekt identiteitsgegevens uit één of meerdere bronnen om ze vervolgens gecontroleerd te kunnen verstrekken aan een verscheidenheid aan doelsystemen. Zie figuur hieronder:

De IAM-functie wordt binnen Kentalis verzorgd door het IAM-systeem. Het IAM-systeem heeft verbindingen met vele systemen binnen het IT-landschap van Kentalis. Deze kunnen worden verdeeld in bronsystemen die informatie aanleveren aan het IAM-systeem en doelsystemen die zijn gekoppeld aan het IAM-systeem op het gebied van rechtentoekenning en/of toegangsvoorziening.

Het HR-systeem is bijvoorbeeld een bronsysteem. Active Directory en Bergop zijn voorbeelden van doelsystemen.



Dit document beschrijft de eisen waaraan een nieuw doelsysteem (applicatie) dient te voldoen om te kunnen worden aangestuurd door het IAM-systeem.

1.1 Toegang (Access management)

Hieronder worden methoden verstaan die worden gebruikt om toegang te krijgen tot een doelsysteem. Kentalis streeft ernaar dat de toegang tot alle doelsystemen door middel van Single sign-on (SSO) wordt gerealiseerd.

1.2 Provisioning

Met de IAM-term ‘provisioning’ wordt bedoeld het transport van gegevens naar het doelsysteem ten behoeve van het aanmaken of afsluiten van een account en het toekennen of intrekken van de juiste autorisaties aan een persoon. Voor het toepassen van provisioning is altijd noodzakelijk dat er ook een methode voor toegang (zie boven) gebruikt wordt.

1.3 Rollen en RBAC

Een in IAM geregistreerde identiteit krijgt, op basis van gegevens uit het bronsysteem, of op basis van een aanvraag, rollen toegekend. Het IAM-systeem kent rechten in het doelsysteem toe op basis van die rollen. Sommige rollen worden automatisch toegekend op basis van attributen van de identiteit, zoals kostenplaats, afdeling of functie. Andere rollen kunnen handmatig toegekend worden op basis van andere eisen die niet in het IAM-systeem zijn af te vangen.

Het toekennen van rollen gebeurt op basis van de autorisatiematrix die wordt opgesteld bij ontsluiting, waarbij de van toepassing zijnde rollen worden gekoppeld aan de rechten in het doelsysteem. De applicatie-eigenaar is verantwoordelijk voor het opstellen, bijhouden en het communiceren van eventuele wijzigingen van de autorisatiematrix.

Een autorisatiematrix geeft dus weer op basis van welke criteria iemand een recht in het doelsysteem krijgt. Criteria zijn liefst automatisch vast te stellen op basis van organisatiegegevens van die medewerker, bijvoorbeeld afdeling of functie. Als dit niet automatisch vast te stellen is, dan moet dit middels een aanvraagbare rol gebeuren. Dat komt ook in de autorisatiematrix te staan.

We kennen de volgende soorten rollen:

- Medewerkerrol
  Basisrol voor alle medewerkers
- Studentrol
  Basisrol voor alle leerlingen
- Functierol
  Toegekend aan iedereen die de betreffende functie bekleed volgens het bronsysteem. Een persoon kan meerdere functierollen hebben.
- Organisatierol
  Toegekend aan iedereen die op de betreffende afdeling werkt. Een persoon kan meerdere organisatierollen hebben.
- Kostenplaatsrol
  Toegekend aan iedereen met die betreffende kostenplaats. Een persoon kan meerdere kostenplaatsrollen hebben.
- Aanvraagbare rol

  Toegekend op basis van een aanvraag, vaak voorzien van een officiële beoordeling.

Voorbeelden:

IAM rol	Roltype	Recht in doelsysteem
MR_medewerker	Medewerkerrol	Recht A
FR_123456 **FR_123457**	Functierol	Recht B
OR_123456	Organisatierol	Recht C
KP_123456	Kostenplaatsrol	Recht D
TR_applicatienaam_rechtE	Aanvraagbare toepassingsrol	Recht E

Als een rol volgens de autorisatiematrix leidt tot een bepaald recht, dan krijgt iedereen met die rol dat recht toegekend. Een recht in een doelsysteem kan bijvoorbeeld een rol, of een groep zijn. Sommige doelsystemen staan slechts één recht per gebruikersaccount toe, andere systemen staan meerdere rechten toe. Indien een systeem één recht toestaat, moet dat expliciet worden aangegeven. IAM staat meerdere rollen per persoon toe en een medewerker kan ook meerdere functie-, organisatie-, kostenplaats- en aanvraagbare rollen hebben.

2 Toegang (access management)

Kentalis maakt voor Single sign-on gebruik van een Identity Provider op basis van Microsoft Entra ID (voormalig Azure AD).

2.1 Mogelijkheden voor het aansluiten Single sign-on (SSO)

Methode	IdP
SAML 2	Microsoft Azure Active Directory
OpenID Connect / OAuth	Microsoft Azure Active Directory

2.2 Aanvraagformulier SSO-koppeling

Het “Aanvraagformulier SSO-koppeling” kan bij Team IAM worden opgevraagd, zodat nieuwe SSO-koppelingen snel gerealiseerd kunnen worden.

2.3 Attributen

Onderstaande attributen zijn beschikbaar voor Single sign-on en Provisioning. Dataminimalisatie is het uitgangspunt, dus attributen worden alleen aangeleverd als ze echt nodig zijn.

Het emailadres van een medewerker of leerling kan wijzigen. Voor unieke identificatie van een identiteit is het nodig het personeelsnummer of studentnummer te gebruiken.

Onderwerp	Regels (voorbeeld)	Medewerker	Leerling	Applicatie
Roepnaam	(Hennie)	J	J	
Initialen	(H.J.)	J		
Voorkeursachternaam	(de Vries)	J	J	
Weergavename	(Vries de, Hennie: [achternaam] <tussenvoegsel>, [roepnaam])	J	J	
Personeelsnummer	(711675)	J		x
Studentnummer	(11065799721)		J	x
Gebruikersnaam	(DVRIESH)	J	J	
E-mailadres	(h.vries@kentalis.nl)	J		
Accountstatus	future, active, grace, inactive, postactive	J	J	
Identiteit type	employee student	J	J	
BRIN	1 waarde, hoofddienstverband voor medewerkers (17GW14)	J	J	
Afdeling	van hoofddienstverband zoals in HR Bronsysteem (90351 ON | VSO Kentalis Compas College SMG - 2)	J		
Functie	van hoofddienstverband zoals in HR Bronsysteem (Onderwijs: Leraar L11, Zorg: Netwerkbeheerder)	J		
Kostenplaats	van hoofddienstverband zoals in HR Bronsysteem (61302 ICT | Connectivity, Infra & netwerk)	J		
Leidinggevende	(cn=VBERGL,ou=employees,ou=active,ou=identities, ou=kentalis,o=resources)	J		

StartVerbintenis	Datum (2017-01-01)	J	J	
EindeVerbintenis	Datum (2099-12-31)	J	J	
Groep	(Hedwig Laout)		J	

Eventuele andere gegevens zijn te leveren als daarvoor een duidelijke doelbinding in het doelsysteem ligt én als deze gegevens beschikbaar zijn in het bronsysteem.

3 Provisioning

Bij de keuze voor provisioning zijn twee zaken van belang: welke methode wordt gebruikt en welke mate van diepgang van provisioning gewenst/mogelijk is. De keuze van de methode en diepgang hangt af van de mogelijkheden van het doelsysteem en de wensen van Kentalis. Hierbij wordt naar de volgende aspecten gekeken:

- Risico: betreft het een doelsysteem die risicovolle informatie bevat
- Omvang: hoeveel mutaties vinden plaats op het gebied van autorisaties en toegang
- Complexiteit:
  - Welke plaats heeft het doelsysteem in de informatiearchitectuur;
  - Wat zijn de (technische) mogelijkheden van het doelsysteem.

3.1 Lijst van eisen

De onderstaande lijst geeft de eisen weer waaraan een doelsysteem dient te voldoen:

- Alle accounts binnen het doelsysteem zijn (via het IAM-systeem) te herleiden naar een uniek persoon. Dit is inclusief beheeraccounts
- Het doelsysteem dient in staat te zijn accounts en de daaraan gerelateerde persoonsgegevens te verwijderen op aangeven van een signaal uit het IAM-systeem
- Het doelsysteem biedt de mogelijkheid om op elk gewenst moment een rapport op te leveren van alle accounts van Kentalis die erin actief zijn of waren en hun actuele autorisaties in het Doelsysteem
- Het doelsysteem verwijdert of anonimiseert persoonsgegevens aantoonbaar uiterlijk 6 maanden nadat de verbintenis met Kentalis is beëindigd.
- **Alle verbindingen tussen het Kentalis IAM-systeem en doelsystemen worden beveiligd door middel van verbindingsbeveiliging, waarvan de minimale specificaties zijn vastgelegd in het cryptografiebeleid van Kentalis[1].**

Bovenstaande eisen en wensen kunnen gebruikt worden voor de beoordeling van een (nieuw) Doelsysteem of als content in een aanbesteding voor een nieuw Doelsysteem.

3.2 Gebruikers/groep/rol provisioning

Voor de provisioning wordt gebruikt gemaakt van het IAM-systeem van Kentalis. Het IAM-systeem kan het volgende leveren:

- Personen (medewerkers en leerlingen)
- Aan de persoon gekoppelde organisatiegegevens (afdeling, functie, locatie , …)
- Van deze gegevens afgeleide groepen, rollen of autorisaties
- Aangevraagde rollen of autorisaties

[1] https://processen.kentalis.nl/iDocument?DocumentId=93a1dc9b-18b3-4e30-a256-7a061aaba594 (alleen interne medewerkers)

3.3 Methode

De volgende methoden van provisioning worden geaccepteerd, waarbij de bovenstaande aspecten richtinggevend zijn:

Naam	Omschrijving	In welke situatie	Techniek
Just-in-time	Op het moment de een persoon zich aanmeldt bij een doelsysteem wordt real time de autorisatiegegevens opgehaald en de juiste rechten gezet. Nadeel: life-cycle kan niet in het doelsysteem aangestuurd worden.	voor Cloud-applicaties waar het hebben van een account en toegangsrechten voorafgaand aan gebruik niet noodzakelijk is	OpenIDConnect
Directe provisioning	Het doelsysteem is direct aan het IAM-systeem gekoppeld en mutaties vanuit het bronsysteem of een aanvraag worden direct doorgevoerd in het doelsysteem.	voor applicaties waarbij het noodzakelijk is dat het account reeds voor gebruik beschikbaar is	(REST)API SCIM JBDC

Alleen als niet gebruik kan worden gemaakt van een van deze twee methode zijn onderstaande methodieken toegestaan:

Naam	Omschrijving	Techniek
Output-/input-provisioning	Mutaties in bronsysteem of aanvragen leiden tot een outputbestand van IAM dat wordt ingelezen en verwerkt in het doelsysteem.	Pick-up bestand (CSV/XML)
Notificatie provisioning	Het doelsysteem kent geen middelen om een geautomatiseerde koppeling te leggen. Het IAM-systeem creëert notificaties die handmatig door de functioneel beheerder in het doelsysteem worden doorgevoerd.	TOPdesk tickets

3.4 Diepgang

Voor de IAM-aansluitvoorwaarden beperken we ons tot twee specifieke type gegevens:

a) Identiteitsgegevens die nodig zijn in het doelsysteem voor het aanmaken van een account.

b) Autorisatiegegevens die in het doelsysteem begrepen worden als een autorisatie.

Afhankelijk van de functionaliteit van het doelsysteem wordt een account aangemaakt op basis van identiteitsgegevens (a) of worden ook de autorisaties binnen de applicatie aangeleverd (b).

Het kan zijn dat bij een doelsysteem die beide vormen van provisioning wenst, twee verschillende methoden worden gebruikt. Bijvoorbeeld directe provisioning voor de identiteitsgegevens en notificatie provisioning voor de autorisatiegegevens.