Van positionering naar conceptueel model – en aandachtspunten ten aanzien van beheer

Identity management in kaart gebracht

Steeds meer bedrijven verdiepen zich in identity management (IdM). Ook steeds meer leveranciers geven aandacht aan IdM-toepassingen. In veel organisaties vraagt men zich momenteel af wat IdM nu precies omvat. Dit artikel geeft in vogelvlucht weer waar IdM binnen de huidige beheermodellen gepositioneerd kan worden. Daarna worden de IdM-oplossingen naar een conceptueel IdM-model vertaald en worden de belangrijkste aandachtpunten ten aanzien van beheer in kaart gebracht.

Bart de Best

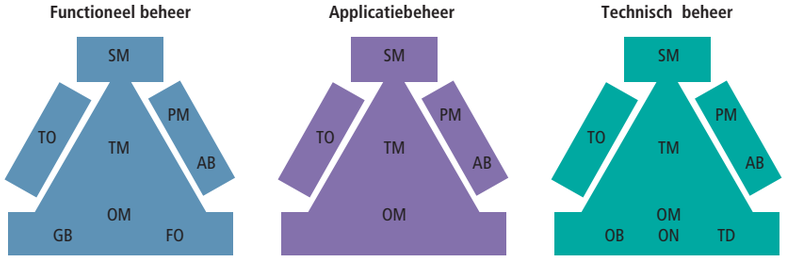
Zoals wel vaker gebeurt met begrippen uit de ICT-wereld, wordt het begrip *identity management* op diverse manieren gedefinieerd en gehanteerd. In dit artikel wordt IdM gezien als een beheerproces. Als uitgangpunt is de definitie van KMPG gehanteerd: "het beleid, de processen en de ondersteunende systemen die bepalen welke personen toegang verkrijgen tot informatie en ICT-middelen en wat iedere persoon gerechtigd is hiermee te doen".

Positionering

Het drievoudig beheermodel van Looijen beschrijft een beheerorganisatie op basis van taakgebieden, taakvelden en taken. De taakgebieden zijn in figuur 1 weergegeven door middel van acroniemen. Een volledige uitwerking van dit model is te vinden in het standaardwerk van Looijen[1].

IdM heeft binnen dit model betrekking op het functioneel beheer, en wel het taakgebied 'gebruikersbeheer' (GB). Hierbinnen vormen het taakveld 'inhoudelijk beheer van bedrijfsgegevens' en de taak 'beheer van autorisatie van gegevensgebruik' het koppelvlak met IdM.

Het model BiSL is vorig jaar gepubliceerd als "een framework voor functioneel beheer en informatiemanagement". Binnen BiSL zijn alleen de IdM-termen *authenticatie* en *autorisatie* terug te vinden binnen het proces 'gebruikersondersteuning'. Beide beheermodellen geven dus aan dat IdM binnen functioneel beheer moet worden gepositioneerd. Veel verder dan het benoemen van de autorisatie komen het drievoudig beheermodel en BiSL echter niet.



Figuur 1 Drievoudig beheermodel (Looijen 2004[1])

Code	Beheertaak	Beschrijving
BBP-2	Beheren autorisaties	Voeren van een autorisatieadministratie en toetsen van autorisatieaanvragen op gestelde eisen. Activeren van de autorisatieaanvragen in de systeemcomponenten (netwerk, servers, applicaties, databases, en dergelijke). Controleren en evalueren van het gebruik van de toegekende autorisaties.
BBPG-3	Beheren gegevens	Zorgdragen voor de actualiteit, integriteit, de volledigheid en het geautoriseerd gebruik van geautomatiseerde gegevensverzamelingen, veelal opgeslagen in databases. Controleren van de naleving van procedures voor correctheid, beveiliging, autorisatie en gebruik van gegevens.

Tabel 1 Taken beheer bedrijfsproces in het NGI-takenmodel

Code	Beheertaak	Beschrijving
BTI-1	Beheren autorisatie- en beveiligings-systemen	Zorgdragen voor de installatie en het optimaal functioneren van autorisatie- en beveiligingssystemen. Instellen van autorisatie- en beveiligingsparameters. Bewaken van het correct functioneren van de autorisatie- en beveiligingssystemen.

Tabel 2 Taak beheer infrastructuur

Het takenmodel van het Nederlands Genootschap voor Informatica (NGI) biedt meer aanknopingspunten. Op het gebied van het 'beheren' van het 'bedrijfsproces' onderkent het NGI een aantal taken, die zijn weergegeven in tabel 1.

Op het gebied van het 'beheren' van de 'infrastructuur' onderkent het NGI de taak in tabel 2.

Om de beheeraspecten van IdM in kaart te brengen bieden deze modellen niet genoeg handvatten. Ze bieden namelijk geen sluitende definitie voor deze vorm van functioneel beheer en geven ook geen invulling aan beheerprocessen, procedures, best practices, et cetera. Andere beheermodellen zoals Application Service Library, ITIL en Cobit doen dit evenmin. Voor de service managers is dit een vervelende situatie: net als bij ketenbeheer moeten zij zelf uitzoeken hoe aan IdM invulling te geven binnen de bestaande beheerkaders.

Daarom moet er eerst een algemeen conceptueel model worden gedefinieerd waarin de diverse IdM-functies van de huidige generatie IdM-oplossingen te vangen zijn. Op basis van dit model is het mogelijk om IdM-beheerkwesties te classificeren en naar generieke oplossingsrichtingen te zoeken.

IdM-gegevensmodel

Om tot een algemeen conceptueel IdM-model te komen, is gekozen voor een logisch IdM-gegevensmodel (*entity relation diagram* (ERD), zie figuur 2) en een IdM-procesmodel (*data flow diagram* (DFD), zie figuur 3). Zie ook kader 'ERD's en DFD's'.

De probleemstelling bij het modelleren van het IdM ERD en het IdM DFD is het gegeven dat er diverse architecturen zijn bedacht om IdM-problemen op te lossen. Eigenlijk zijn er dus net zoveel IdM ERD's en DFD's te definiëren als er IdM-architecturen (lees: huidige-generatie-IdM-oplossingen) zijn. Om toch een generiek conceptueel gegevensmodel neer te zetten is besloten om redundantie in de modellen op te nemen. Deze is te herkennen aan de kleuren blauw, groen en grijs (zie figuur 2). Deze kleuren geven de verschillende autorisatiemethoden aan, die onder 'IdM-functies' beschreven worden.

In het IdM-gegevensmodel zijn onder meer de volgende entiteittypen te onderscheiden:

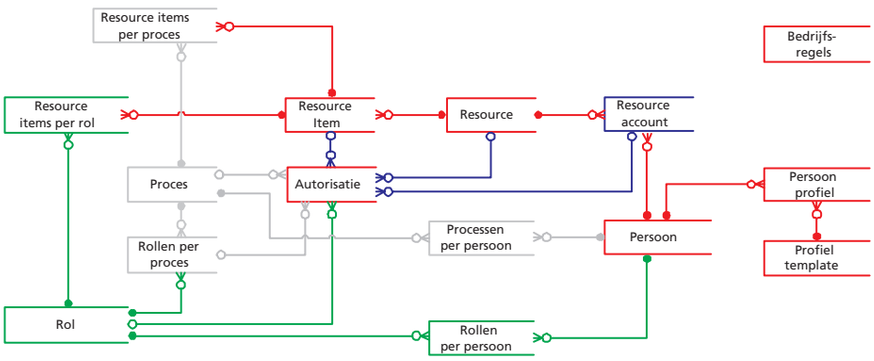
Bedrijfsregels: een IdM-bedrijfsregel (business rule) schrijft voor aan welke eisen de IdM-informatie en het gebruik van de informatie moeten voldoen.

Persoon: een medewerker van een bedrijfsproces of beheerproces. IdM-oplossingen bieden de mogelijkheid om personen binnen IdM te definiëren in de vorm van een IdM-account. Dit is dus een generiek account waaraan rechten voor rollen en/of processen kunnen worden toegekend. Ter onderscheid hiervan wordt het traditionele account voor een resource in dit model resource account genoemd.

Persoon profiel: de profielgegevens die behoren bij een persoon, zoals de nieuwsgroep die aan de persoon is gekoppeld.

Proces: zowel bedrijfsprocessen, het beheerproces als zelfs externe processen.

Topic is de studierubriek in *IT Beheer Magazine*, waarin een actuele ontwikkeling of een belangrijk onderdeel van het vakgebied diepgaand wordt belicht.
In nummer 9/2005 (bladzijde 45) heeft Bart de Best de business case beschreven voor identity management. Dit artikel brengt het concept van identity management in kaart.



Figuur 2 IdM ERD: entiteittypen van IdM

Profiel template: een set van eigenschappen die toegekend wordt aan een persoon om de informatie die getoond moet worden aan een persoon te personaliseren.

Resource: een ICT-dienst of ICT-product met functies waarmee gegevens gemanipuleerd kunnen worden. De relaties die voor resource items gelden, zijn ook van toepassing op resources.

Resource account: een registratie van een persoon of een resource. Een persoon kan meerdere resource accounts hebben.

Resource item: een module of onderdeel van een resource, bijvoorbeeld een applicatiemodule.

Rol: een beschrijving van een set van bij elkaar horende taken.

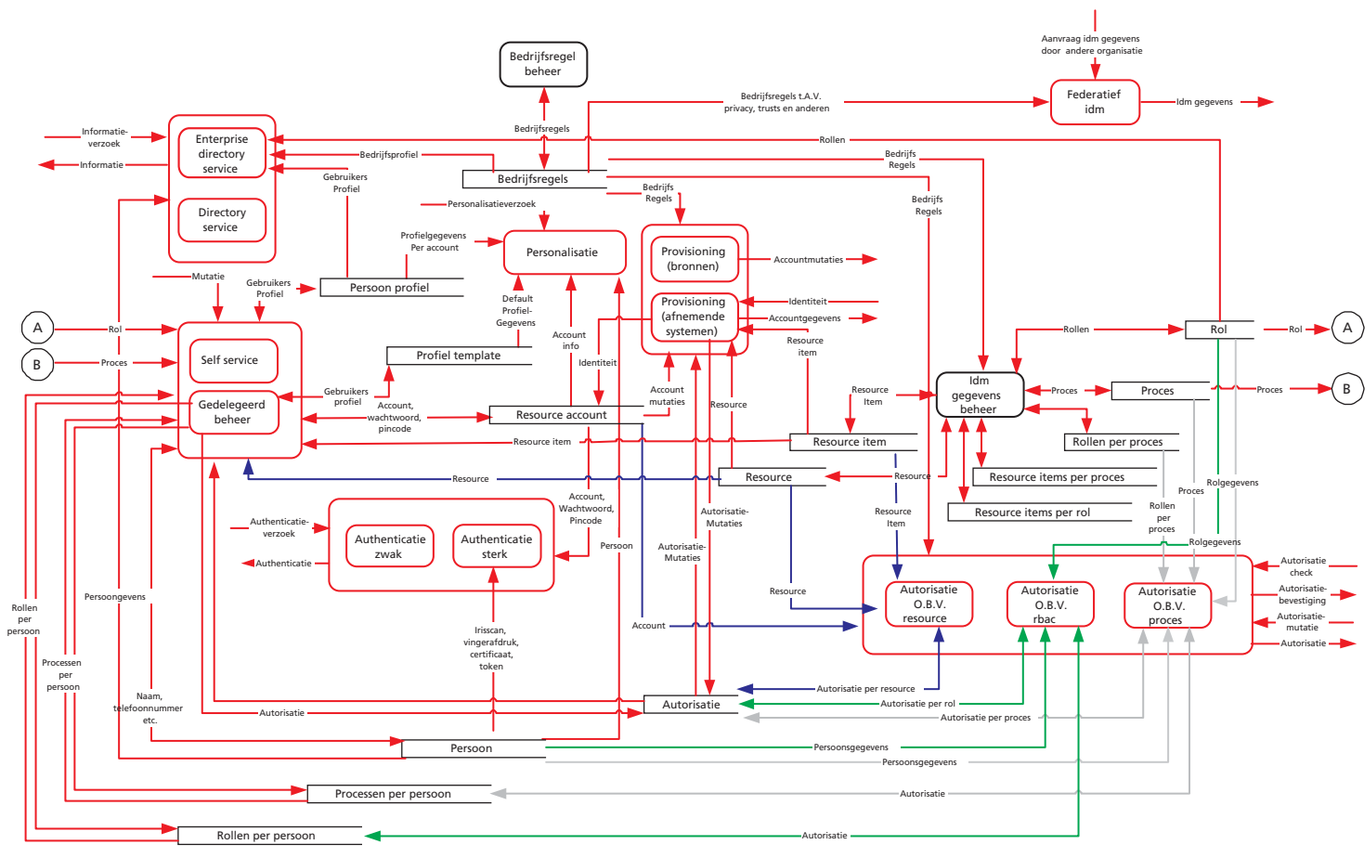
Rollen per proces: rollen die aan een proces kunnen worden toegekend. Hierdoor is het mogelijk om autorisaties toe te kennen aan rollen binnen een bepaald proces.

IdM-procesmodel

Alhoewel het ERD een model is waarin de complete informatiebehoefte van het IdM-proces is ondergebracht, geeft dit nog niet een compleet beeld van de IdM-functionaliteit. Zo zegt het definieren van een entiteittype als 'persoon' niets over de wijze waarop een persoon geauthentiseerd wordt. Hiervoor moet naar het gebruik van deze IdM-gegevens worden gekeken, met andere woorden: de IdM-functies.

De meest voorkomende IdM-functies waaruit het IdM-proces bestaat zijn: authenticatie, autorisatie, personalisatie, provisioning, gedelegeerd beheer, self-service, directory service en federatief identity management. Deze IdM- functies zijn als rode ovalen in het DFD afgebeeld en zijn gerelateerd aan de entiteittypen van het IdM ERD. De zwarte ovalen zijn beheerfuncties die moeten worden ingericht om de bedrijfsregels, processen en rollen die door de IdM-functies gebruikt worden, te beheren. Ten behoeve van de overzichtelijkheid geeft het DFD voor de functie federatief IdM niet alle informatiestromen weer.

De beschrijving hierna van de IdM-functies is onder andere gebaseerd op het rapport 'Identity Management in het Hoger Onderwijs'[2].



Figuur 3 IdM DFD: IdM-functies gerelateerd aan entiteittypen

ERD en DFD

Een entity relation diagram (ERD) is een logische beschrijving van de gegevens die in een database kunnen worden vastgelegd en opgevraagd. Het ERD beschrijft dus het geheugen van de IdM-functies. De entiteittypen (gegevensverzamelingen) zijn weergegeven als open rechthoeken. Een pijl geeft de relatie aan tussen twee entiteittypen. Een pijl met een open rondje staat voor een optionele relatie en een gesloten rondje voor een verplichte relatie. Een drietand geeft aan dat er sprake is van een 1:N-relatie. Zo kan een persoon meer rollen hebben en kan een rol aan meer personen zijn toegekend.

Een data flow diagram (DFD) is een logische beschrijving van de IdM-functionaliteit. De rechthoeken zijn ontleend aan het ERD. De pijlen zijn de informatiestromen die nodig zijn om een IdM-functie uit te voeren. Elke ovaal geeft een IdM-functie weer. Een ovaal *in* een ovaal geeft aan dat een IdM-functie op meerdere manieren geïmplementeerd kan worden. Zo kan de authenticatie zwak of sterk zijn. Een informatiestroom die aansluit op de buitenste ovaal staat voor een generieke input/output van gegevens. Zo hebben beide IdM-implementaties van authenticatie informatie van een 'resource account' nodig. Een informatiestroom die rechtstreeks naar een ovaal binnen een ovaal gaat, duidt op een specifieke informatiebehoefte. Zo heeft alleen een sterke authenticatie-implementatie de gegevens van een persoon nodig.

Authenticatie
Deze functie heeft tot doel om vast te stellen dat een persoon degene is die hij zegt te zijn. Hiertoe worden zowel zwakke als sterke authenticatiemethoden onderkend. De zwakke is de oude vertrouwde account-wachtwoordcombinatie. Sterkere authenticatiemethoden gebruiken een token of certificaat dat als attribuut aan het entiteittype persoon gekoppeld kan worden. De sterkste methode is die waarbij een toetsing plaatsvindt op wat alleen de persoon *weet* (pincode/wachtwoord), wat de persoon *bezit* (hardware-token) en wat de persoon *kenmerkt* (irisscan, vingerafdruk).

De efficiëntiewinst die met veel IdM-oplossingen kan worden behaald, is het eenmalig authenticeren van een gebruiker tijdens het inloggen, single sign-on (SSO) genaamd. Dit wordt ook wel reduced sign-on (RSO) genoemd, omdat honderd procent SSO praktisch gezien vaak onhaalbaar is. Bij RSO vormt IdM een soort van middleware die 'onder water' de authenticatie tot alle te gebruiken resources verzorgt, zoals applicaties, databases, netwerken, et cetera. Een bijzondere vorm van SSO is die van webapplicaties. Deze zogenaamde Web SSO handelt alle authenticaties af binnen één browsersessie.

Autorisatie
Deze functie heeft tot doel om vast te stellen of een persoon of systeem recht heeft op de aangevraagde onderdelen van de resource(s) (resource items). Historisch gezien zijn er drie autorisatiemethoden te onderscheiden, die elk een ander entiteittype als uitgangspunt hebben. Elke methode heeft in het ERD en het DFD een andere kleur.

Resource (blauwe lijnen): van oorsprong is autorisatie gebaseerd op de combinatie van een resource account plus wachtwoord. De blauwe lijnen geven deze relatie weer. De autorisaties worden verleend per resource of resource item.

Rol (groene lijnen): de huidige generatie IdM-oplossingen gebruikt een dynamischere koppeling van resources en resource accounts, door het definiëren van rollen. Dit wordt dan ook de Role Based Access Control (RBAC) genoemd. Een rol geeft een persoon rechten op bepaalde resources. Het wel of niet toekennen van een rol aan een persoon geschiedt op basis van een zogenaamde bedrijfsregel (business rule).

Proces (grijze lijnen): het nadeel van op RBAC gebaseerde IdM-oplossingen is dat dit zoveel uitzonderingsregels met zich meebrengt. De rollen zijn goed voor tachtig procent van de autorisaties. De resterende twintig procent vergt echter dat er allerlei handmatige uitzonderingsregels in zo'n IdM-oplossing moeten worden gedefinieerd en onderhouden. Een alternatief is het scheiden van de rollen en autorisaties door middel van processen. Door autorisaties aan de relatie van een proces en een rol te koppelen ontstaat een veel generieker autorisatiemodel.

Overigens is het niet altijd vereist om geauthentiseerd te zijn alvorens geautoriseerd te kunnen worden. Er zijn bijvoorbeeld technieken waarbij een netwerkadres van een werkplek ook goed genoeg is, zoals bijvoorbeeld toegepast in routers.

Personalisatie
Het doel van deze functie is het afstemmen van de soort en vorm van ICT-dienst en -informatievoorziening op persoonlijke kenmerken zoals afdeling, functie, locatie, et cetera.

Centraal bij het personaliseren van diensten en informatie staat het gebruikersprofiel (persoonsprofiel). Naarmate de personalisatie complexer wordt, nemen ook de beheerinspanningen toe. Een goede ondersteuning in de zin van IdM-oplossingen is dan ook raadzaam.

Vaak wordt er onderscheid gemaakt tussen personalisatie door de gebruiker zelf (customization) en die vanuit de organisatie. Voorbeelden van customization zijn de aanpassingen die de gebruiker aanbrengt binnen zijn werkblad. Personalisatie vanuit de organisatie is bijvoorbeeld het wel of niet beschikken over een applicatie-icoon op het werkblad op basis van de functie van de gebruiker.

Provisioning
Dit heeft tot doel het automatisch aanmaken, aanpassen en verwijderen van

	Autorisatie	Bedrijfsregels	Persoon	Persoon profiel	Proces	Processen per persoon	Profiel template	Resource	Resource account	Resource item	Resource Items per Proces	Resource items per rol	Rol	Rollen per persoon	Rollen per proces
Authenticatie (sterk)			R						R						
Authenticatie (zwak)									R						
Autorisatie (resource)	CRUD	R						R	R	R					
Autorisatie (proces)	CRUD	R	R		R	CRUD			R				R		R
Autorisatie (RBAC)	CRUD	R	R						R				R	CRUD	
Bedrijfsregelbeheer		CRUD													
Directory service			R												
Enterprise directory service		R	R	R									R		
Federatief IdM	R	R	R						R						
(Gedelegeerd) beheer	CRUD		CRUD	CRUD		CRUD	CRUD	R	CRUD	R			R	CRUD	
Personalisatie			R	R			R		R						
Provisioning (afnemend systeem)	CRUD	R						R	CRUD	R					
Provisioning (bron)	R	R							R						
IdM-gegevensbeheer		R			CRUD			CRUD		CRUD	CRUD	CRUD	CRUD		CRUD
Selfservice	R		RU	RU	R	R		R	CRUD	R			R	R	

Tabel 3 IdM-levenscyclus

identiteitgegevens in andere systemen teneinde beheerkosten te reduceren. Informatiesystemen en andere resources zoals besturingssystemen maar ook routers bevatten informatie over wie wat mag doen. Veel van deze producten voorzien niet in een externe authenticatie- en autorisatiemethode zoals integrated security. Hierbij zijn credentials (identiteitgegevens) die bij het inloggen op het netwerk verkregen zijn, ook afdoende om de lokale autorisatie te verrichten.
Het zou de voordelen van IdM teniet-doen om deze systemen handmatig bij te werken voor elke mutatie in de IdM-database. Daarom bieden de meeste IdM-oplossingen de faciliteit om deze identiteitgegevens in andere systemen automatisch aan te passen. Uiteraard is dit een belangrijke voorwaarde voor RSO.

Provisioning is een noodzakelijk onderdeel van IdM-oplossingen om efficiënt beheer mogelijk te maken of RSO te kunnen realiseren. Hierbij wordt een onderscheid gemaakt tussen *afnemende systemen* en *bronnen*. Bij afnemende systemen worden identiteiten in resource accounts voor gebruikers vertaald. Bij bronnen worden gebruikersidentiteiten aangemaakt. Typische bronsystemen zijn het personeelssysteem en CRM-systemen (bijvoorbeeld voor externe relaties). Bij deze laatste vorm van provisioning, die ook wel account provisioning wordt genoemd, is rolgebaseerde toegangscontrole van belang. Als de rechten van de gebruikers in kaart zijn gebracht, dienen de accounts voor de gebruiker immers alleen in die systemen te worden aangemaakt waar deze krachtens zijn rol toegangsrechten toe heeft.

Gedelegeerd beheer en selfservice
Het doel hiervan is het verstrekken van rechten om IdM-beheertaken uit te laten voeren door decentrale beheerorganisaties of de gebruiker zelf, teneinde de werklast te verdelen en de accuraatheid van de IdM-gegevens te verhogen.

Van oudsher is het beheren van personen en hun rechten geen sinecure. De meeste organisaties boekhouden personen vele malen in verschillende systemen. Het is dan ook enorm veel werk en de gegevens zijn vaak niet accuraat. Neem bijvoorbeeld de kwaliteit van de gegevens in een servicedesktool. Sommige bedrijven hebben dit functioneel beheerprobleem ingeperkt door bruggen te slaan tussen informatiesystemen. Andere bedrijven hebben gekozen voor het beleggen van deze administratie bij decentrale organisaties of zelfs bij de gebruikers zelf. Met de mogelijkheid van gedelegeerd beheer en selfservice is binnen IdM-oplossingen rekening gehouden met deze verscheidenheid aan organisatie-inrichtingen. De gegevens blijven centraal opgeslagen worden, en ook blijft centraal bepaald worden wie welke gegevens mag beheren.

Directory service
Deze functie heeft als doel: het centraal definiëren, vastleggen en toegankelijk stellen van persoonsgegevens.

Deze service biedt een overzicht van personen en persoonsgegevens. De techniek stamt al uit de jaren tachtig, en in de afgelopen decennia hebben deze 'elektronische telefoonboeken' zich sterk ontwikkeld, inclusief protocollen. Zo heeft Microsoft er zijn Active Directory omheen gebouwd en opengesteld met het LDAP-protocol. Veel IdM-oplossingen maken dankbaar gebruik van deze centrale opslag van persoonsgegevens.

Contingency-factor	Authenticatie	Autorisatie	Directory service	Provisioning	Personalisatie	Selfservice	Gedelegeerd beheer	Federatief IdM
Overheid	Code Tabaksblat WBP	Code Tabaksblat WBP	WBP					WBP
Buitenland	SOX Bazel II	SOX Bazel II						
Infrastructuur				Heterogene componenten				
Aandeelhouders	Vraag naar inzicht beveiliging en compliancy	Vraag naar inzicht beveiliging en compliancy						
Leveranciers	IdM-tools	IdM-tools	IdM-tools	IdM-tools	IdM-tools	IdM-tools	IdM-tools	IdM-tools
Consumenten			Vraag naar informatie	Vraag naar SSO/RSO	Vraag naar informatie op maat	Vraag naar flexibiliteit	Vraag naar autonomie	Vraag naar toegankelijk-heid
Afnemers							Vraag naar flexibiliteit	Vraag naar ondersteuning procesintegra-tie
Concurrenten	Informatie-beveiliging	Informatie-beveiliging						Informatieuit-wisseling
Actiegroepen	Beveiliging tegen terreur	Beveiliging tegen terreur						
Financiers	Vraag naar efficiëntie	Vraag naar efficiëntie	Fusies en globalisering vereisen inzicht					Vraag naar efficiëntie

Tabel 4 Contingencyfactoren van Pascoe-Samson[3]

IdM kan de gegevens in een directory verrijken met rollen, profielen, bedrijfsprofielen (policy's), et cetera. Ook kunnen metagegevens opgenomen worden over identiteitsgegevens uit een aantal andere directory's. In beide gevallen spreekt men dan ook wel van een *enterprise directory*.

Federatief identity management
Doel hiervan is het toegankelijk maken van IdM-functies over bedrijven heen ter ondersteuning van afgesproken elektronische diensten.

Steeds meer bedrijven fuseren, werken samen of hebben van overheidswege een informatie-uitwisseling. Dit is geen nieuw fenomeen. De intensiteit en complexiteit van de samenwerking van de bedrijfsprocessen is echter wel nieuw. Er bestaat dan ook steeds meer behoefte aan IdM-functies over organisaties heen. Dit wordt federatief IdM genoemd. Uiteraard zijn IdM-gegevens vertrouwelijk, al was het maar vanwege de Wet Bescherming Persoonsgegevens op dit gebied. Daarnaast is er vanuit concurrentieoverwegingen natuurlijk ook de nodige voorzichtigheid met het uitwisselen van IdM-gegevens. Hiervoor moet dus een goed filter gedefinieerd worden. Het doel van de meeste organisaties bij federatief IdM is dan ook functies over organisaties heen te definiëren voor authenticatie, autorisatie en personalisatie, zonder de identiteit van de betrokken personen vrij te geven.

IdM-CRUD-analyse

Nu het IdM-gegevensmodel (ERD) en het IdM-procesmodel (DFD) uiteen zijn gezet, is een volledigheidscheck mogelijk door te controleren of elke gegevensverzameling (entiteittype) volledig beheerd wordt. Dit kan door middel van een zogenaamde CRUD-analyse (create – read – update - delete). Een dergelijke CRUD voor de IdM-gegevens is opgenomen in tabel 3.

Hiermee is de gehele levenscyclus van alle IdM-gegevens in kaart gebracht en op volledigheid gecontroleerd. Behalve voor een compleetheidanalyse is de CRUD natuurlijk ook prima geschikt om snel te zien welke IdM-functie welke IdM-gegevens beheert. Overigens moet gesteld worden dat de CRUD voor federatief IdM sterk afhankelijk is van de bedrijfsregels. De CRUD in tabel 3 geeft voor deze IdM-functie de meest gebruikte informatie weer, maar een afwijkende invulling is dus heel goed mogelijk.

IdM-functies: drijfveeranalyse

Het conceptuele IdM-model (ERD+DFD) biedt meer functionaliteit dan de traditioneel onderkende functionaliteit op het gebied van toegangsbeheer en gebruikersbeheer. Voor het uitbreiden van de IdM-functionaliteit moet echter een drijfveer aanwezig zijn die de investering rechtvaardigt (business case). In de matrix in tabel 4 zijn mogelijke drijfveren voor IdM-functies aangegeven per *contingencyfactor* (externe beïnvloedingsfactor, Pascoe-Samson[3]). De volgende contingencyfactoren zijn niet van toepassing gebleken: het milieu, het weer, de media, de werknemersorganisatie, de consumentenorganisatie, omwonenden en de werkgeversorganisaties.

IdM-functies: beheerissues

Bij het inrichten van (extra) IdM-functies is het belangrijk om naar de gerelateerde beheeraspecten te kijken. Vaak wordt gesteld dat een IdM-project voornamelijk (voor zestig procent) gericht is op het beheer. Tabel 5 geeft per IdM-functie zowel de drijfveren als voorbeelden van beheerissues.

Ook zijn de volgende algemene beheerissues te onderkennen:

- Het IdM-systeem is een informatiesysteem op zich; dat vraagt om continuiteit en beveiliging. Daarnaast zal het opslaan van audit trails veel opslagcapaciteit vergen.
- De beheerder van de technische IdM-systemen moet niet in staat zijn om 'via de achterdeur' de regels te omzei-

IdM-drijfveren	IdM-functie/invulling van drijfveren	IdM-beheerissues
Wet- en regelgeving zoals SOX, WBP, Code Tabaksblat vereisen rapportage.	Authenticatie/ Centralisatie van authenticatie informatie in IdM tools. Sterke authenticatie die persoonsgebonden is.	Sterke authenticatie vereist veel innovatie van ICT middelen.
Terreurdreiging vereist beveiliging.		Legacysystemen zijn niet altijd goed met IdM-tools te integreren.
Wet- en regelgeving zoals SOX, WBP, Code Tabaksblat vereisen rapportage.	Autorisatie/ Centralisatie van autorisatie informatie in IdM tools. Vereenvoudiging van het autorisatie model door autorisatie op rollen te baseren (RBAC). Autorisatie op proces niveau.	Vereist een koppeling van alle betrokken resources met IdM- tool.
Terreurdreiging vereist beveiliging.		Definitie van rollen en toekenning aan functionarissen.
		Granulariteit van rollen is te hoog, uitzonderingen moeten handmatig toegekend worden.
		Bedrijfsprocessen moeten inzichtelijk zijn voor IT-organisatie.
Organisaties worden groter door globalisering. Toegankelijkheid van informatie wordt steeds belangrijker.	Directory service/ Enterprise Directory Services ontsluiten belangrijke informatiebronnen.	Verstrekte informatie moet goed beveiligd zijn. (Niet) beschikbaar zijn van het IdM-systeem heeft een grote invloed op de business continuity.
Globalisering vereist integratie van IdM-functies tussen bedrijven.	Federatief IdM/ Federatief IdM is een nieuw fenomeen.	Privacy moet gewaarborgd blijven.
Wetgeving zoals WBP vereist afscherming van gegevens.		
Door informatietoename raken communicatielijnen verstopt.	Personalisatie/ Resourceonafhankelijke personalisatie zoals bij portal services. Personalisatie op groepsniveau.	Per applicatie moet dit enabled worden. Er moet in policy's opgenomen worden wie welke informatie mag inzien.
Gebruikers vereisen vereenvoudiging van resourcetoegang. E-commerce, globalisering, et cetera vereisen dat steeds meer gebruikers over meer resources beschikken.	Provisioning/ Provisioning naar afnemende systemen vanuit bronnen.	Legacysystemen staan dit lang niet altijd toe. Elke afnemer van de IdM- gegevens moet alleen zijn eigen subset krijgen. Hiervoor moeten filters gedefinieerd worden. Lang niet iedereen mag over alle IdM-gegevens beschikken. Naast een functioneel filter moet er dus ook een beveiligingsfilter gedefinieerd worden. Dit kan zelfs een wettelijke eis zijn.
Gebruikers vereisen vereenvoudiging in omgang met ICT-middelen, zoals minder keren aanloggen.	Selfservice/ reduced sign-on	Trainen van gebruikers.
		Kwaliteit van de gegevens moet geborgd worden. Ontlasting van de (ICT-)helpdesk voor bijvoorbeeld het resetten van wachtwoorden.
ICT-middelen inbedden in organisatie. Gebruikers willen meer autonomie in het beheer van IdM-gegevens.	Gedelegeerd beheer	Herdefiniëren van taken, verantwoordelijkheden en bevoegdheden.
	Bedrijfsregelbeheer	
	Rollenbeheer	

Tabel 5 Beheerissues per IdM-functie

len (bijvoorbeeld: MS SQL 6.5 bood een technisch beheerder de mogelijkheid om als Super User op de database in te loggen via de console, ook al had hij het wachtwoord niet).

- Het onderhouden van rollen en functies in de organisatie moet belegd worden als continue activiteit. Periodieke herziening volstaat niet meer.
- Rollenbeheer en bedrijfsregelbeheer zijn zaken die in veel organisaties niet expliciet zijn belegd, laat staan uitgeschreven. Dit omdat men vaak 'vreest' voor claims van medewerkers die vinden dat bepaalde bevoegdheden en/of verantwoordelijkheden bij hun rol horen. Zolang men die rollen ondoorzichtig houdt, kunnen medewerkers ze niet opeisen. IdM gaat hiervoor een 'bedreiging' vormen.

De in tabel 5 opgesomde beheerissues en de generieke beheerissues zijn alleen indicatief en dus niet limitatief, met andere woorden: het is mogelijk dat zich in de praktijk andere beheerkwesties voordoen. Om te komen tot een effectief en efficiënt IdM-proces moeten de beheerissues per organisatie volledig in kaart worden gebracht en voorzien worden van oplossingen.

In een artikel later in deze jaargang zal Bart de Best een aanpak voor IdM-projecten publiceren.

Drs. ing. Bart de Best RI is werkzaam als service manager bij Qforce B.V.

Noten

1 Looijen, M., *Beheer van informatiesystemen*, ten Hagen & Stam Uitgevers/SDU Uitgevers, 2004
2 IdM-begrippen: http://aaa.surfnet.nl/info/artikel_content.jsp?objectnumber=57992
3 Pascoe-Samson, E., *Organisatie: besturing en informatie*, ten Hagen & Stam Uitgevers/SDU Uitgevers, 2003

Met dank aan Rob Waterlander voor de review, en Willem van Dis, IdM-consultant bij ManageID, voor zijn medewerking aan dit artikel.