STARTERKIT IDENTITY MANAGEMENT

versie 1.0, 4 april 2011

SURFNET BV, RADBOUDKWARTIER 273, POSTBUS 19035, 3501 DA UTRECHT
T +31 302 305 305, F +31 302 305 329, WWW.SURFNET.NL

INHOUD

1. Inleiding 4
1.1 Aanleiding 4
1.2 Doelstelling 4
1.3 Doelgroep 4
1.4 Werkwijze en leeswijzer 4
2. Definitie identity management 6
3. De vijffasenaanpak identity management (managementsamenvatting) 7
3.1 Aanleiding ontwikkeling vijffasenaanpak 7
3.2 Waarom de gekozen volgorde? 8
3.3 Fase 1: Definitie 8
3.4 Fase 2: Beleid 9
3.5 Fase 3: Architectuur en processen 9
3.6 Fase 4: Infrastructuur 10
3.7 Fase 5: Implementatie 10
4. Deelactiviteiten fase 1: Definitie 11
4.1 Projectinitiatie 11
4.2 Aanleiding / probleemstelling 11
4.3 Afstemming met organisatiedoelen 13
4.4 Hoofddoelen / voordelen (ambitie) 14
4.5 Omvang en reikwijdte IdM-project (scope) 15
4.6 Roadmap (beknopt overzicht van het IdM-programma) 16
4.7 Inrichten projectorganisatie 16
4.8 Inrichten beheerorganisatie 18
4.9 Tot slot 19
5. Deelactiviteiten fase 2: Beleid 20
5.1 Detailafbakening beleid IdM 20
5.2 Uitgangspunten en randvoorwaarden 20
5.3 Beleid voor de onderdelen van IdM 20
5.4 Relevante wet- en regelgeving 23
5.5 Tot slot 23
6. Deelactiviteiten fase 3: Architectuur en processen 24

6.1 Beschrijving informatiearchitectuur voor IdM-omgeving 24
6.2 Functionele beschrijving IdM-processen (businesslaag) 25
6.3 Beschrijving IdM-processen 26
6.4 Gap-analyse: van huidige naar gewenste situatie 27
6.5 Tot slot 28
7. Deelactiviteiten fase 4: Infrastructuur 29
7.1 Definiëren componenten en standaarden 29
7.2 Beschrijving noodzakelijke technische aanpassingen (doelarchitectuur) 30
7.3 Selectie producten en diensten 31
7.4 Gap-analyse technische infrastructuur 32
7.5 Tot slot 32
8. Deelactiviteiten fase 5: Implementatie 33
8.1 Organisatorische aanpassingen 33
8.2 Implementatie basisinfrastructuur 33
8.3 Implementatie tactisch niveau 33
8.4 Uitvoeren acceptatietests 34
8.5 Inproductiename 34
8.6 Oplevering IdM-project 34
8.7 Tot slot 34

1. INLEIDING

1.1 Aanleiding

In 2008 is geïnventariseerd hoe ver instellingen in het hoger onderwijs en onderzoek zijn op de gebieden informatiebeveiliging, identity management en security incident management. De inventarisatie heeft aangetoond dat op de genoemde gebieden nog verbetering mogelijk is door het delen van best practices en het 'normeren' van de te volgen aanpak. Dit heeft geleid tot het opstellen van starterkits en leidraden op deze drie gebieden.

De aanleiding voor het opstellen van een starterkit identity management is dat instellingen vaak wel hun techniek op orde hebben, maar dat dit regelmatig geen verband heeft met de aanwezigheid van beleid of zelfs niet met de aanwezige procesbeschrijvingen. Daarnaast zien veel instellingen op tegen de invoering van identity management vanwege de breedte van het beslag op de organisatie.

Deze starterkit betreft met name het opstellen van beleid en het onderhoudbaar maken van de architectuur en procesbeschrijvingen. Deze zaken dragen bij aan een betere governance met behulp van identity management.

1.2 Doelstelling

Deze starterkit is bedoeld om instellingen in het hoger onderwijs en onderzoek handvatten te geven bij het inrichten van het identity management binnen hun organisatie, waarbij ook aandacht geschonken wordt aan de hierboven genoemde tekortkomingen.

1.3 Doelgroep

De doelgroep van deze starterkit is de afdeling Informatiemanagement en ICT-managers, waar doorgaans het eerst het besef doordringt dat de huidige wijze waarop identity management is georganiseerd de nodige knelpunten kent.

In tweede instantie vormen ook systeemhouders, eigenaren van bron- en doelsystemen, decentrale beheerders, de security officer en interne auditors een belangrijke doelgroep. Zij zijn degenen die het succes van een gestructureerde en gestroomlijnde aanpak van identity management mogelijk kunnen maken en, samen met de eindgebruikers, daarvan ook de voordelen plukken.

1.4 Werkwijze en leeswijzer

In dit document wordt ingegaan op de organisatie van identity management en een projectmatige aanpak daarbij. Daarin worden vijf fasen onderscheiden, die achtereenvolgens doorlopen moeten worden.

Kern van deze aanpak is dat identity-managementprocessen en –techniek pas in tweede instantie aan bod komen. Er wordt gestart met een definitiefase, waarin op organisatieniveau een aantal zaken aan bod komen, zoals de verhouding van identity management tot de doelstellingen van de gehele instelling. Vervolgens wordt expliciet aandacht besteed aan het beleid m.b.t. identity management. Hier valt veel

efficiencywinst te behalen, als het lukt om over de gehele organisatie de vertaling van het beleid naar rollen en processen te stroomlijnen. Pas daarna wordt gekeken naar de informatiearchitectuur, de benodigde techniek en de implementatie ervan.

In hoofdstuk 3 wordt het overall-beeld geschetst van de gefaseerde projectaanpak voor identity management; dit hoofdstuk kan daarom ook beschouwd worden als een managementsamenvatting. In de hoofdstukken 4 t/m 8 wordt voor elk van de vijf fasen apart de aanpak met bijbehorende deelactiviteiten iets uitgebreider toegelicht.

Voordat de procesmatige aanpak wordt behandeld, geven we eerst in hoofdstuk 2 een korte definitie van identity management.

2. DEFINITIE IDENTITY MANAGEMENT

Om te bereiken dat de starterkit door iedereen op dezelfde wijze wordt geïnterpreteerd, geven we eerst kort de gebruikte definitie van identity management en de daarin gehanteerde basisbegrippen.

Identity management (IdM), ook wel Identity & Access Management (IAM) genoemd, is het geheel van beleid, processen en techniek voor het beheer en gebruik van elektronische identiteitsgegevens en wordt gebruikt om alle vormen van authenticatie en autorisatie te faciliteren.

Elektronische identiteitsgegevens zijn de elektronisch vastgelegde gegevens die gebruikt worden om vast te stellen wie de gebruiker is en of hij geautoriseerd is voor datgene wat hij elektronisch wil doen, bijvoorbeeld toegang verkrijgen tot een bedrijfsnetwerk of een EPD inzien.

Beleid is het aangeven van de richting en de middelen waarmee het management de gestelde doelen van IdM wil gaan realiseren.

De processen die bij IdM gebruikt worden, zijn (zie ook bijlage 1: begrippenlijst):

- **identificatie**: jezelf kenbaar maken door het verstrekken van officiële persoonsgebonden kenmerken, zoals een paspoort of rijbewijs;
- **provisioning**: geautomatiseerd doorgeven van nieuwe, gewijzigde en verwijderde identiteitsgegevens, vaak inclusief authenticatiegegevens, naar applicaties en diensten met het doel efficiënt en consistent gebruikersbeheer te bewerkstelligen;
- **authenticatie**: laten zien dat je beschikt over op persoonlijke basis verstrekte of geverifieerde gegevens of eigenschappen die horen bij een bepaalde account en identiteit;
- **autorisatie**: verkrijgen van bepaalde bevoegdheden, die bij de persoon behoren, mogelijk op basis van rollen of op basis van andere criteria.

Een van de aspecten die tijdens het IdM-proces ‘geregeld’ moet worden is het life cycle management van identiteiten en rollen: hoe wordt omgegaan met nieuwe en vertrekkende personen en personen die van functie of taak veranderen?

De techniek die een rol speelt bij IdM is ondersteunend aan de genoemde processen.

3. DE VIJFFASENAANPAK IDENTITY MANAGEMENT (MANAGEMENTSAMENVATTING)

3.1 Aanleiding ontwikkeling vijffasenaanpak

Voor een IdM-project wordt vaak een technische insteek gekozen, zonder dat er is nagedacht over de inbedding van IdM in de organisatie. Dat leidt veelal tot ad-hocoplossingen, grote verschillen in benadering tussen faculteiten, afdelingen en diensten, geen afstemming met de strategische organisatiedoelen, kortom tot veel inefficiënties.

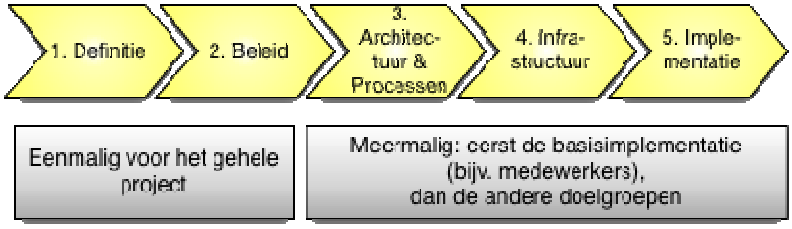
Veelgehoorde redenen om nog eens naar de opzet en inrichting van IdM in een instelling voor hoger onderwijs en onderzoek te kijken, zijn:

- Personen hebben meerdere identiteiten (voor verschillende toepassingen).
- Het duurt weken voordat een account is aangemaakt.
- Er is een vervuilde en verouderde administratie van verleende autorisaties.
- Er is voor iedere student een licentie aangeschaft, maar men weet niet hoeveel studenten er daadwerkelijk gebruik van maken.
- De herleidbaarheid van handelingen in geautomatiseerde systemen is niet gewaarborgd.
- Men weet niet of de Wet Bescherming Persoonsgegevens goed is geïmplementeerd is en of men ‘in control’ is.
- Personen hebben allerlei toegang die zij niet hoeven te hebben en dat brengt risico’s met zich mee van (on)bewuste inbreuk op de integriteit en vertrouwelijkheid van gegevens.
- Er is weinig zicht op wat exact is geïmplementeerd.

Samengevat komen de redenen om IdM te verbeteren neer op de wens een of meer van de volgende doelen te realiseren:

- verbeterde gebruiksvriendelijkheid;
- meer tijdigheid, correctheid en volledigheid;
- betere kostenbeheersing;
- betere veiligheid;
- aantoonbaar verbeterde privacy;
- betere compliance;
- grotere beheersbaarheid / betere onderhoud systematiek;
- betere stroomlijning door de organisatie.

Kern van de vijffasenaanpak is dat IdM-processen en –techniek pas in tweede instantie aan bod komen (zie onderstaande figuur).



Steeds vaker blijkt dat er een duidelijke business case is voor deze aanpak; de te behalen efficiencywinsten kunnen groot zijn.

Hieronder wordt de vijffasenaanpak toegelicht.

3.2 Waarom de gekozen volgorde?

De keuze voor deze opeenvolgende fasen is ingegeven door een aantal overwegingen:

Aansturing

De aansturing van IdM moet niet vanuit de techniek gebeuren, maar vanuit het College van Bestuur en de gebruikersorganisatie. Daarnaast moet de uitvoering binnen de kaders van de wet en de doelen van de organisatie moet plaatsvinden.

Immers, een puur technische aanpak gaat voorbij aan het belang van IdM voor de gehele instelling en haar missie en leidt bovendien in te geringe mate tot stroomlijning en efficiencyverbetering voor alle organisatieonderdelen. De technische benadering leidt er niet toe dat IdM wordt ingebed in de organisatie (missie, strategie, beleid). Daarom is het noodzakelijk dat de uiteindelijk verantwoordelijke bestuurders zich op hoofdlijnen committeren.

Beleidsdoelen

De hoofddoelen van beleid moeten centraal vastgelegd worden. Daarbij zijn afstemming met organisatiedoelen (alignment op strategisch niveau en het maken van onderhoudbare procesbeschrijvingen) belangrijke elementen.

De integrale top-down benadering maakt het mogelijk de gewenste aansturing en beleidsformulering te realiseren.

3.3 Fase 1: Definitie

De definitiefase van een IdM-project heeft tot doel het project in te bedden in de onderwijsinstelling en haar omgeving en op hoofdlijnen richting te geven aan het project.

Daarbij gaat het om de volgende onderdelen:

- aanleiding / probleemstelling: welk(e) knelpunt(en) moeten worden opgelost;
- alignment: op welke manier draagt het IdM-project bij aan het bereiken van de organisatiedoelen;

- bestuurlijk commitment;
- wat is de scope en ambitie van het project: hoofddoelen en reikwijdte;
- roadmap: projectaanpak op hoofdlijnen;
- inrichten projectorganisatie.

3.4 Fase 2: Beleid

Onder beleid verstaan we het aangeven van de richting en de middelen (processen en ondersteunende systemen) waarmee het management de gestelde doelen wil gaan realiseren, veelal in een vooraf benoemde tijd. Vaak wordt onderscheid gemaakt tussen hoofddoelen en tussendoelen, die bedoeld zijn om een deel van het hoofddoel te bereiken.

In de beleidsfase gaat het om:

- detailafbakening beleid IdM: wat willen we nu precies bereiken;
- (eventueel) benoemen van uitgangspunten en randvoorwaarden: inhoudelijk of in financiële zin;
- beleid voor de hoofdonderdelen van IdM: identificatie, life cycle management, authenticatie, autorisatie, beheer van IdM-systemen, rapportage en audits en kwaliteit;
- beschrijving rollenmodel en aansluitvoorwaarden;
- relatie met relevante wet- en regelgeving.

3.5 Fase 3: Architectuur en processen

Als het beleid is geformuleerd, kan het vertaald worden naar een globale architectuur en bijbehorende processen.

Onderdelen van deze fase:

- beschrijving informatiearchitectuur: de bronsystemen en hun gewenste relatie met de doelsystemen;
- beschrijving van de onderliggende processen t.b.v. functioneel en technisch beheer in drie lagen:
  1. functionele of businesslaag;
  2. applicatielaag;
  3. datalaag;
- inrichten van het mechanisme om deze architectuur- en procesbeschrijvingen goed te onderhouden bij wijzigingen;
- gap-analyse ‘gewenst versus bestaand’: bepalen welke aanpassingen nodig zijn om de gewenste situatie te bereiken.

3.6 Fase 4: Infrastructuur

In de infrastructuurfase gaat het om de volgende onderdelen:

- definitie van componenten en standaarden: systemen voor authenticatie en autorisatie (LDAP, AD), koppelingen (DB, SOAP, federatie, enzovoort) en single sign-on servers;
- beschrijving van de doelarchitectuur: welke technische aanpassingen zijn noodzakelijk;
- opstellen van de eisen en wensen voor producten en diensten: leidt tot productkeuze, noodzakelijk voor technische realisatie;
- opstellen van het inproductiename-plan: met migratiescripts en acceptatietests.

3.7 Fase 5: Implementatie

Bij de uitvoering van het inproductiename-plan gaat het om:

- organisatorische aanpassingen: samenwerking tussen organisatieonderdelen;
- implementatie van de basisinfrastructuur: server- en software-infrastructuur voor IdM;
- uitvoeren van acceptatietests: om te toetsen of het gewenste effect bereikt wordt; eventueel zaken bijstellen;
- verdere implementatie: gebruikersbeheer, toegangsbeheer, life cycle management, beveiliging, het beheer van de rollen, en dergelijke;
- inproductiename: leidt tot werkend IdM-systeem, inclusief provisioning;
- overdragen van het projectresultaat naar beheerorganisatie / ICT-afdeling.

4. DEELACTIVITEITEN FASE 1: DEFINITIE

In de definitiefase komen de volgende deelactiviteiten aan de orde:

1. projectinitiatie;
2. aanleiding / probleemstelling;
3. afstemming met organisatiedoelen (alignment);
4. hoofddoelen / voordelen (ambitie);
5. omvang en reikwijdte IdM-project (scope);
6. roadmap (aanpak op hoofdlijnen);
7. inrichten projectorganisatie;
8. inrichten beheerorganisatie.

4.1 Projectinitiatie

De meest natuurlijke afdeling bij een hogeronderwijsinstelling om een IdM-project te initiëren is Informatiemanagement. Dat komt omdat de problematiek van IdM op bijna alle organisatieonderdelen betrekking heeft en daarom een organisatiebrede aanpak vereist met een strategisch karakter.

Naast projectinitiator is de afdeling Informatiemanagement de trekker van de volledige fasen 1 Definitie en 2 Beleid van deze aanpak. De informatiemanager moet daarbij nauw samenwerken met de functioneel beheerder, die de contacten met alle stakeholders onderhoudt.

Onderdeel van de projectinitiatie is het verkrijgen van commitment van het topmanagement voor het IdM-project. Veelal gaat dat iteratief gedurende de gehele definitiefase. Het achterwege laten van het verkrijgen van commitment van het College van Bestuur kan leiden tot vroegtijdige afbreuk van het project door gebrek aan budget en tot een gebrek aan aansturing en eensgezindheid bij betrokkenen: een mandaat kan dus zeer nuttig zijn.

4.2 Aanleiding / probleemstelling

Medewerkers en studenten zijn tegenwoordig gewend om overal en altijd toegang te hebben tot ICT-toepassingen en ze verwachten dat het toegangsproces eenvoudig en eenduidig is. Impliciet verwachten de gebruikers ook dat er zeer zorgvuldig wordt omgegaan met inloggegevens en dat de toegangsrechten op de juiste manier zijn ingesteld. De privacy van de gebruiker en de vertrouwelijkheid van gegevens moeten zijn gewaarborgd.

Deze verwachtingen vragen om een strak gecoördineerd beheer van inloggegevens, toegangsrechten en een goede bescherming van persoonlijke data.

Daarnaast verwachten gebruikers in het hoger onderwijs en onderzoek steeds vaker dat deze zaken ook over de instellingsgrenzen heen goed zijn geregeld. Dit vraagt om een nog grotere beheerinspanning van inloggegevens, toegangsrechten en privacy.

Dit probleem is uiteraard niet uniek voor het hoger onderwijs en onderzoek, maar is een probleem waar veel grote organisaties tegenaan lopen. Een goede oplossing is om de toegang tot toepassingen meer centraal te regelen en gebruikers zoveel mogelijk toegang te verschaffen op basis van kenmerken die specifiek zijn voor een organisatie. Het is gebruikelijk om het bestaan van accounts te koppelen aan de status van een individu in het personeelssysteem of het studenteninformatiesysteem.

Sinds ongeveer tien jaar wordt deze aanpak identity management genoemd en sinds enige tijd zijn er ook goede softwareoplossingen op de markt die IdM ondersteunen. Alle universiteiten en hogescholen zijn bezig om IdM in te richten of te verbeteren.

Veel gehoorde redenen om IdM te willen introduceren of verbeteren zijn:

- Iedere ICT-toepassing heeft een eigen inlogsystematiek, waardoor medewerkers en studenten zeer veel wachtwoorden moeten onthouden. Dit leidt tot verhoogde kans op slordigheden en verlies.
- Het duurt weken voordat een account (eventueel handmatig) is aangemaakt;.
- Het beheer van accounts is tijdrovend en verzoeken aan de helpdesk om verloren wachtwoorden te vervangen zijn legio.
- De instelling heeft geen idee of de Wet Bescherming Persoonsgegevens op een goede manier geïmplementeerd is.
- Er is voor iedere student een licentie aangeschaft voor (bepaalde) software, maar men weet niet hoeveel daarvan gebruik maken.

Een goede analyse van het probleem dat met IdM moet worden opgelost helpt bij de bepaling van de oplossing ervan. De formulering van beleidsdoelen kan als volgt gaan (7 stappen):

1. Wat is het probleem?

Om beleid te kunnen maken, moet je eerst het probleem helder in kaart brengen.

2. Hoe maak je aannemelijk dat dit probleem echt bestaat?

Zorg ervoor dat je het bestaan van het probleem kunt aantonen, bijvoorbeeld met resultaatoverzichten.

3. Wat wil je met stap 1?

Zeg duidelijk:

a) dat je wat je in stap 1 hebt waargenomen ongewenst vindt, en

b) dat je het tegenovergestelde ziet als gewenste situatie. Beschouw dat als het streefbeeld, de plek waar je ooit zou willen uitkomen. Dat is dus een (politiek) waardeoordeel.

4. Waarom wil je dat?

Beargumenteer expliciet waarom je een gewenste situatie wil. Zonder redengeving hangt het waardeoordeel in de lucht.

5. Wat is de oorzaak van het probleem?

Analyseer de oorzaken van het probleem (omgevingsanalyse). Alleen als je die kent, kun je tot een fundamentele oplossing komen.

6. Welke oorzaken pak je aan?

Weeg af welke oorzaken je met succes kunt aanpakken.

7. Wat ga je concreet doen?

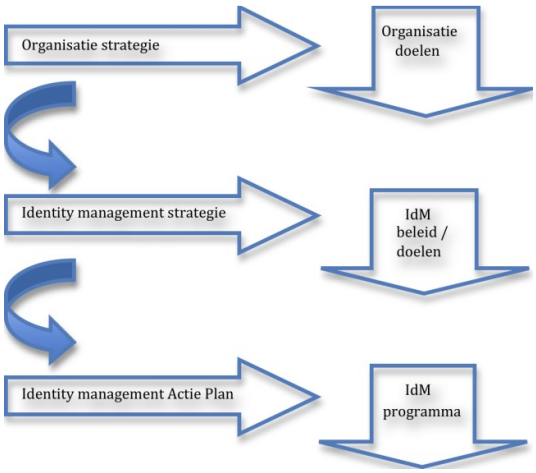
Als je weet welke oorzaken je gaat aanpakken om het probleem op te lossen, formuleer dan de concrete acties die een bijdrage moeten leveren aan het naderbij brengen van de gewenste situatie zoals die is geformuleerd in stap 3b.

Door een dergelijke exercitie uit te voeren, wordt voorkomen dat er een 'oplossing' wordt verzonnen voor een niet bestaand probleem of voor een onjuist benoemd probleem. Nu sluit je aan bij de oorzaken van een onderbouwd knelpunt. Daarmee is in feite ook je ambitie op hoofdlijnen bepaald. In bijlage 2 wordt een voorbeeld uitgewerkt voor het doorlopen van deze stappen.

4.3 Afstemming met organisatiedoelen

Het is om diverse redenen verstandig om de relatie tussen IdM en het overall beleid van een organisatie te leggen. Beschrijf daarbij hoe IdM bijdraagt aan het bereiken van de doelen van de organisatie (alignment). Dat geldt overigens ook voor andere deelterreinen dan IdM, zoals informatiebeveiliging, personeelsbeleid, financiën, milieu, enzovoort.

Onderstaande afbeelding is een schematische voorstelling van de 'vertaling' van organisatiedoelen naar IdM-doelen en programma:



Door de afstemming van het IdM-beleid met de overall-doelstelling van de organisatie wordt aangetoond dat de implementatie van IdM helpt om de organisatiedoelen te bereiken (kwalitatief dan wel kwantitatief). Dit zal op voorhand zeker behulpzaam zijn bij discussies met het College van Bestuur of de directie over nut en noodzaak van

investeren in IdM en ook in allerlei discussies achteraf over compliance met wet- en regelgeving en 'corporate governance'.

In de onderwijssector speelt tevens een rol dat er over de organisatiegrenzen heen steeds vaker wordt samengewerkt. Het is dan belangrijk elkaars ICT-beleid en de steeds belangrijker eisen, zoals 'always-on' en de implicaties daarvan voor veiligheid te kennen.

4.4 Hoofddoelen / voordelen (ambitie)

IdM regelt de volgende zaken:

A. Gebruiksvriendelijkheid

- De gebruiker heeft één gebruikersnaam en wachtwoord voor alle diensten en applicaties van de instelling en hoeft slechts op één daarvan in te loggen om daarna alle toepassingen te kunnen gebruiken. Uitzonderingen zijn (onderdelen van) applicaties die een grotere veiligheid vereisen dan gemiddeld. Daar worden andere, sterkere, inlogmiddelen gebruikt (denk bijvoorbeeld aan de methoden bij internetbankieren).
- Gebruikers kunnen door middel van een webinterface hun wachtwoorden wijzigen of resetten, mailaliassen kiezen en hun werklocatie wijzigen als ze intern verhuisd zijn.
- Gebruikers kunnen met hun inlognaam en wachtwoord van de instelling ook inloggen bij andere instellingen en bij diensten van derden, zoals bij uitgevers.

B. Compliance

- Door middel van uniforme processen voor aanmaken, wijzigen en verwijderen van accounts en de bijbehorende toegang maakt IdM het beter mogelijk om te voldoen aan kwaliteitsnormen en wettelijke richtlijnen voor het omgaan met privacygevoelige gegevens.
- IdM kan rapportages opleveren die van belang zijn voor audits die accountants uitvoeren.

C. Beheersbaarheid

- IdM is een mix van beleid, processen en techniek. Door deze drie componenten expliciet te beschrijven en de beschrijvingen goed te onderhouden (in lijn met de implementatie), wordt de uitgifte van accounts en toegang beheersbaar gemaakt.
- Kostenbesparing:

  IdM biedt kostenbesparing op de volgende punten:

  a. Handmatige invoer van accounts in ICT-toepassingen is niet meer nodig; nieuwe toepassingen kunnen eenvoudig aansluiten op de gerealiseerde IdM-infrastructuur. De ICT-toepassingen krijgen de juiste gegevens voor toegang en inloggen aangeleverd via een proces dat provisioning wordt genoemd.
  b. Het probleem- en incidentbeheer ten aanzien van wachtwoorden en toegangsrechten neemt af.
  c. Door het slim uitdelen van rechten kan op termijn mogelijk bespaard worden op softwarelicentiekosten.

De invoering van IdM kan worden aangegrepen om verschillen in soortgelijke processen voor verschillende applicaties, afdelingen, etc. op te heffen en daarmee meer uniformiteit en eenvoudiger beheer rondom accounts en rechten te bewerkstelligen.

D. Veiligheid en privacy

- De privacy van gebruikers neemt toe omdat hun persoonlijke kenmerken en inloggegevens vanuit één centrale plek worden beheerd. Dat is veiliger dan dat deze verspreid in de organisatie en zonder samenhang worden bewaard, waardoor de kans op ongewenste openstelling of fraude een stuk groter wordt omdat de kwaliteit van het beheer niet kan worden gecontroleerd. De kwaliteit kan wel gecontroleerd / geborgd worden bij centraal beheer.
- Omdat gebruikers nog maar één wachtwoord hoeven te onthouden, zijn ze beter te stimuleren om een lastig te raden wachtwoord te kiezen en er zorgvuldig mee om te gaan.

Uit dit overzicht van doelen / voordelen die met IdM gerealiseerd kunnen worden, zijn de mogelijk te behalen doelen voor een specifieke organisatie duidelijk af te leiden. Leg deze doelen duidelijk vast en zorg voor afstemming daarvan met de organisatiedoelen.

De meest gehoorde redenen om (weer) iets aan IdM te doen zijn op dit moment compliance ("we kunnen niet aantonen dat we voldoen aan relevante wet- en regelgeving") en kostenbeheersing ("de huidige situatie van IdM in onze instelling wordt gekenmerkt door een versnipperde aanpak, die leidt tot onbeheersbare kosten"). Stroomlijning van definities en processen (zie hierboven) kan in de laatste situatie tot forse efficiencywinsten leiden.

4.5 Omvang en reikwijdte IdM-project (scope)

Omdat het ondoenlijk is om voor alle ICT-toepassingen en alle soorten gebruikers in één project het IdM-systeem in te richten – want zo'n project zou erg omvangrijk zijn en nooit af komen -, wordt er vaak gewerkt met deelprojecten. Die deelprojecten samen worden ook wel het IdM-programma genoemd. Bij het bepalen van de scope van het IdM-programma (en de onderliggende deelprojecten) is het verstandig om te beschrijven welke ICT-toepassingen en welke gebruikers daar wel en niet onder vallen.

Het meerjarige IdM-programma zou zich kunnen uitstrekken over de gehele digitale leer- en werkomgeving van een instelling (bijvoorbeeld kantoorautomatisering, e-mail, Blackboard, digitale bibliotheek, intranet en content management systeem) en zou dan de ICT-toepassingen die daarvoor gebruikt worden aangaan, plus studenten, alumni, medewerkers en derden. De financiële systemen bijvoorbeeld vallen dan niet onder het IdM-programma.

De diverse projecten die als onderdeel van het programma worden uitgevoerd zullen meestal betrekking hebben op alle personen die kunnen inloggen op ICT-systemen, maar het is goed om ook te kijken naar categorieën die nu misschien nog niet, maar in de toekomst wel moeten kunnen inloggen: scholieren, alumni, medewerkers en studenten van andere instellingen (via de SURFfederatie), etc.

Het IdM-systeem levert in technische zin vaak een mooi middlewaresysteem op dat gebruikt kan worden voor uitwisseling en doorsturen van aan personen gerelateerde gegevens tussen ICT-systemen, maar evengoed voor andere gegevens. Uit het oogpunt van beveiliging en privacy is het vaak verstandig om daartussen een logische scheiding aan te maken en het IdM-systeem bijvoorbeeld te beperken tot aan personen gerelateerde gegevens voor authenticatie, autorisatie en communicatie.

Ook deze fase is belangrijk richting CvB en andere stakeholders. Tijdig inzicht in wat wel en wat niet onder het project valt is van belang voor de verwachtingen die zij over het project hebben. Deze moeten goed gemanaged worden; communicatie is hierbij erg belangrijk. Om die reden wordt ook de roadmap ontwikkeld.

4.6 Roadmap (beknopt overzicht van het IdM-programma)

Met het beschrijven van de roadmap wordt beoogd inzicht te geven in de projectaanpak op hoofdlijnen. Een roadmap is minder expliciet qua planning, kosten en resultaten. Dit is een belangrijk instrument van verwachtingsmanagement richting stakeholders; het voorkomt vervelende verrassingen voor hen tijdens de vervolgfasen.

Naast algemeen verwachtingsmanagement als reden voor het opstellen van een roadmap is daar ook een budgettaire reden voor. Het is lastig om van te voren een goede inschatting te maken van de exacte kosten die later in deelprojecten gemaakt moeten worden om het overall projectplan uit te voeren in de daarvoor geraamde doorlooptijd. Daarom is het verstandig om in de roadmap een globale raming van kosten en doorlooptijden per projectfase op te nemen en ervoor te zorgen dat vóórdat elke nieuwe fase gestart wordt, deze globale raming vervangen wordt door een goed onderbouwde raming van kosten en doorlooptijden van de betreffende fase. Wees zo verstandig om in de roadmap duidelijk aan te geven wat het bekostigingmodel is per projectfase. Komt het budget uit de algemene (ICT-)middelen, of wordt verwacht dat de afdelingen een bijdrage in de kosten leveren.

Het helpt om per globaal benoemd deel project in de roadmap duidelijk te beschrijven wat de deliverables zijn en aan welke kwaliteitseisen die moeten voldoen. Daarmee wordt ook duidelijk hoe de deel projecten zich ten opzichte van elkaar verhouden.

Ook hier geldt dat (financieel) verwachtingsmanagement cruciaal is voor het welslagen van het project. Als de roadmap langs deze lijnen beschreven is, dan kan op basis daarvan de projectorganisatie worden ingericht.

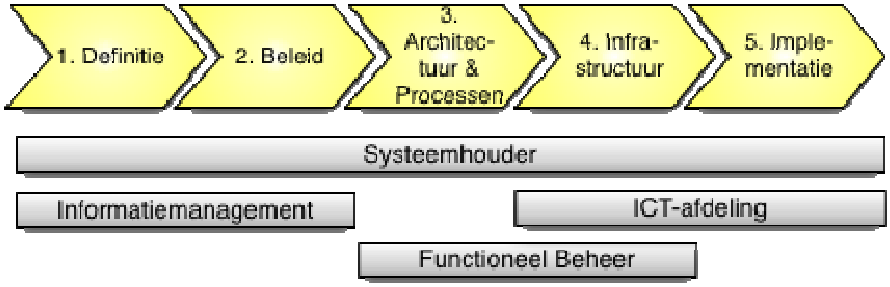
4.7 Inrichten projectorganisatie

Voordat een project gestart kan worden, zijn er al enkele zaken aan de orde geweest, vaak in discussie met het management: wat is het probleem, wat worden we er beter van, welke ambitie hebben we, wat is de relatie van het project met de overall doelstelling van de instelling, wat wordt de scope van het project, is er een business case, wat zijn de alternatieven, etc. Dergelijke discussies moeten uiteindelijk leiden tot een goedgekeurd projectplan met bijbehorend budget. In een goed projectplan wordt ook aandacht geschonken aan de communicatie met degenen die met de uitkomst van het project te maken krijgen.

Een goed ingerichte projectorganisatie kent in elk geval de volgende onderdelen:

1. formele opdrachtverlening aan het project- of programmamanagement;
2. goedgekeurd projectplan, inclusief de benodigde 'middelen';
3. bemensing projectorganisatie;
4. eigenaarschap en documentbeheer;
5. communicatie- en rapportagestructuur.

De aansturing van een IdM-project moet niet vanuit de techniek gebeuren, maar vanuit betrokkenheid van alle belanghebbenden. Deze zijn per onderscheiden fase:



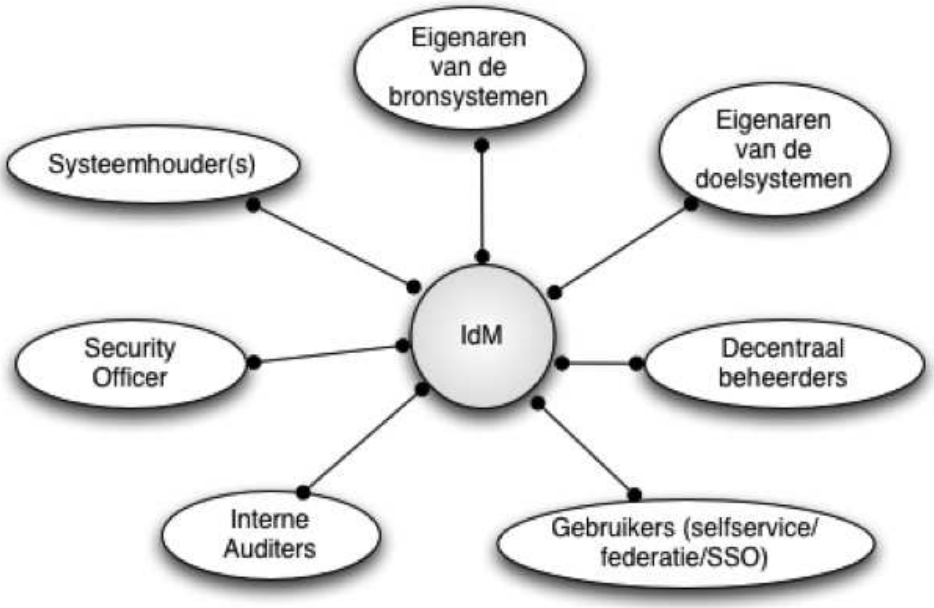
Informatiemanagement is de initiator van het project, omdat dit een organisatiebreed onderwerp is dat niet lager (op operationeel niveau) in de organisatie belegd kan worden. De informatiemanager draagt zorg voor de formulering van het beleid. Dit doet hij in nauwe afstemming met de functioneel beheerder.

De functioneel beheerder draagt zorg voor de beschrijving van de architectuur en de IdM-processen en voor de afstemming met de hieronder benoemde stakeholders. De architectuur en processen moeten in lijn zijn met het beleid.

De systeemhouder is de eigenaar van het IdM-systeem. Deze moet zorgen voor het aantonen van nut & noodzaak van (verbeterde) IdM binnen de instelling. Dat kan door aan te tonen dat (verbeterd) IdM bijdraagt aan het realiseren van de organisatiedoelen (alignment). Ook het financieringsmodel voor het IdM-project is zijn taak. Daarbij zie je vaak dat de basisinfrastructuur gefinancierd wordt uit het centrale (ICT-)budget, en dat het aansluiten van de doelsystemen decentraal gefinancierd wordt door de diverse eigenaren van en belanghebbenden bij doelsystemen. Tenslotte is de operatie van het IdM-systeem de verantwoordelijkheid van de systeemhouder.

De ICT-afdeling zorgt voor de beschrijving van de applicatie en het technisch beheer.

Bij het inrichten van de projectorganisatie moeten alle stakeholders betrokken zijn. Het gaat hierbij in elk geval om de volgende betrokken functionarissen:



Bij een IdM-project moet gedacht worden aan minimaal de volgende deelnemers:

- projectleider: vaak het hoofd van de afdeling Informatiemanagement;
- projectsecretariaat: medewerker Informatiemanagement of elders vandaan;
- relevante proceseigenaren, zoals HR, IT-beheer, financiën, studentenadministratie, e.d.;
- security officer;
- communicatie.

Daarnaast zullen er rapportages aan de opdrachtgever verzorgd moeten worden m.b.t. de voortgang en het beheer (tijd, geld, kwaliteit, informatie en organisatie) van het project.

4.8 Inrichten beheerorganisatie

Een groot deel van de projectorganisatie gaat na afloop van het project over in de beheerorganisatie. De focus komt daarbij meer te liggen op de decentrale beheerders en de gebruikers. Van belang is dat de beschreven methodiek (vooral de rollen en processen) goed onderhoudbaar is. Daarvoor verantwoordelijk is de functioneel beheerder. Wijzigingsverzoeken worden aan hem/haar gericht en worden besproken in het gebruikersoverleg. Het is belangrijk dat de basisdefinities en -processen door de gehele organisatie zoveel mogelijk dezelfde blijven (stroomlijning daarvan was immers een van de drijvers voor verbetering van het IdM-systeem; zie ook paragraaf 4.4 hoofddoelen / voordelen). Wel kunnen lokaal aanvullingen of kleine wijzigingen worden ingevoerd die de basisdefinities en –processen niet ‘overhoop’ halen.

4.9 Tot slot

Veel IdM-projecten worden gestart vanuit de techniek, zonder aandacht te besteden aan de voorafgaande fasen, waarvan de definitiefase de eerste vormt. Kort gezegd komt deze fase er op neer dat het programma wordt ingebed in de organisatorische en beleidssetting van de instelling, waardoor het management en beheer van het project in de organisatie belegd zijn. Dit heeft grote voordelen voor de instelling.

Als de definitiefase goed doorlopen is, zijn de volgende deliverables gerealiseerd:

- Commitment van topmanagement;
- IdM-strategie en –ambitie in lijn met organisatiedoelen;
- formele projectorganisatie met benoemde rollen en verantwoordelijkheden;
- budget, mensen en andere middelen, gerelateerd aan roadmap (inclusief het bekostigingsmodel);
- communicatie- en rapportageplan;
- inbedding van het projectbeheer in de organisatie.

5. DEELACTIVITEITEN FASE 2: BELEID

In de beleidsfase komen de volgende deelactiviteiten aan de orde:

1. detailafbakening beleid IdM;
2. uitgangspunten en randvoorwaarden;
3. beleid voor de onderdelen van IdM;
4. beschrijving IdM-beheer;
5. relevante wet- en regelgeving;

5.1 Detailafbakening beleid IdM

Fase 1: in de definitiefase is op hoofdlijnen aangegeven wat wel en wat niet onder het IdM-project valt.

Fase 2: de beleidsfase biedt de mogelijkheid om dit meer in detail uit te werken. De detailafbakening van IdM-beleid kan eruit bestaan dat bepaalde uitzonderingen benoemd worden, bijvoorbeeld: 'in het IdM-project wordt niet gekeken naar processen waarbij slechts enkele vaste medewerkers betrokken zijn, zoals de Afdeling Financiën'. Of: 'de toegang tot de resultaten van 'research voor marktpartijen' wordt gescheiden georganiseerd van het IdM-systeem voor studenten en medewerkers'.

Het expliciteren hiervan is belangrijk in het licht van verwachtingsmanagement en de aantoonbaarheid van zaken, zoals het voldoen aan wet- en regelgeving. Ook de interne accountant zal er blij mee zijn.

5.2 Uitgangspunten en randvoorwaarden

Niet in elk project is aandacht voor de beleidsuitgangspunten en zijn randvoorwaarden een issue. Maar vaak moet het project passen binnen een groter raamwerk en dat wordt dan als beleidsuitgangspunt benoemd. Bijvoorbeeld "het IdM-project moet passen binnen de vastgelegde kaders voor de universitaire informatievoorziening en mag niet strijdig zijn met het beleid m.b.t. privacy en informatiebeveiliging".

Soms worden er financiële randvoorwaarden gesteld. Bijvoorbeeld: "de vernieuwing van het IdM-systeem binnen de hogeschool komt voor rekening van het algemene ICT-budget, de uitvoering daarvan zal gefinancierd worden door de diverse proceseigenaren en de faculteiten die voor de uitvoering verantwoordelijk zijn". Voor zover deze zaken niet al in de definitiefase zijn bepaald, moet dat hier gebeuren.

5.3 Beleid voor de onderdelen van IdM

Beleid is het aangeven van de richting en middelen (processen en ondersteunende systemen) waarmee het management (over een bepaald tijd gezien) de gestelde doelen wil gaan realiseren.

De gestelde doelen van IdM zijn (op hoofdlijnen) al bepaald in fase 1 (definitie). Indien gewenst kunnen deze hoofddoelen hier verder worden uitgewerkt en toegelicht, maar strikt noodzakelijk is dat niet.

In deze paragraaf gaat het om de richting en middelen waarmee de doelen gerealiseerd moeten worden binnen de organisatie en met behulp van techniek. Bij IdM worden doorgaans de volgende beleidsonderdelen onderscheiden: identificatie, life cycle management, authenticatie, autorisatie, beheer van IdM-systemen, rapportages & audits en kwaliteitsbeleid.

Voor elk van deze beleidsvelden moeten beschreven worden wat er onder verstaan wordt. Onderstaand een voorzet voor de belangrijkste beleidsvelden:

Identificatie

Identificatie is het vaststellen van de juiste identiteit van een persoon en het daarna koppelen van een of meerdere authenticatiemiddelen aan die persoon.

Identificatie kan op verschillende manieren plaatsvinden:

- in een inlogscherm invoeren van een gebruikersnaam of user id
- gebruik van een vingerafdruk of een ander biometrisch kenmerk
- gebruik van een token (een smartcard of een ander apparaatje, zoals een usb-stick).

Het identificatiebeleid moet minimaal omvatten voor welke objecten een persoon zich behoort te identificeren, met behulp van welke systematiek dat moet plaatsvinden (gebruiksnaam / user id, token, e.d., eventueel verschillend per object) en wie het identificatiebeleid onderhoudt en vaststelt.

Life cycle management

Life cycle management bestaat uit processen en alle onderliggende techniek voor het aanmaken, beheer en gebruik van elektronische identiteitsgegevens.

Het life cycle management beleid moet in elk geval bevatten hoe omgegaan wordt met de creatie, verrijking, toepassing en verwijdering van identiteiten en bijbehorende accounts van de verschillende doelgroepen (rollen). Vaak wordt in het hoger onderwijs gewerkt met de (hoofd)rollen medewerker, student, alumni en derde.

Authenticatie

Bij authenticatie laat u zien dat u beschikt over een authenticatiemiddel dat hoort bij een bepaalde account en identiteit.

De identiteit is vooraf op een andere manier vastgesteld (identificatie). Het doel van de authenticatie is om te laten zien dat gebruiker is wie zij/hij zegt te zijn, maar strikt genomen kan alleen worden vastgesteld dat een gebruiker tijdens de authenticatie het bij een identiteit horende authenticatiemiddel heeft gebruikt.

Het authenticatiebeleid moet minimaal omvatten welke authenticatiemiddelen worden gebruikt, om welke reden, wie het beleid onderhoudt en vaststelt.

Autorisatie

Autorisatie is het proces van het verlenen van toegang aan personen of systemen tot (delen van) de functionaliteit van ICT-diensten. Idealiter zijn voor autorisatie geformaliseerde bedrijfsregels opgesteld waaraan de identiteit van de gebruiker moet voldoen om toegang tot diverse omgevingen te verkrijgen.

Het autorisatiebeleid moet in elk geval bevatten wie bepaalt hoe de toegang geregeld is (verantwoordelijkheden). Daarbij kan onderscheid gemaakt worden naar doelgroepen, classificatie van informatie, soorten authenticatie, maatregelen bij vermeend misbruik en rapportages, auditing en alertering.

Beheer van IdM-systemen

Voor het beheer van IdM-systemen zullen uitgangspunten, verantwoordelijkheden en rollen moeten worden vastgelegd. Voor elk systeem (bron of doel) moet beschreven worden wie de eigenaar ervan is, door wie en hoe veranderingen worden doorgevoerd en welke beleidsuitgangspunten daarbij toegepast worden.

Van belang is hoe omgegaan wordt met veranderingen in de systemen; die zullen volgens een vooraf bepaalde methodiek moeten worden behandeld en gedocumenteerd. In de vorige paragraaf is een plaatje getoond voor hoe de organisatie rondom IdM in een projectfase is. Een dergelijke taakverdeling kan ook voor operationeel beheer worden vastgesteld.

Deze beschrijving van het IdM-beheer moet bovendien zelf ook onderhouden worden; veranderingen in verantwoordelijkheden en beleidsuitgangspunten moeten worden doorgevoerd. Het resultaat is een up-to-date beschrijving, die de feitelijke situatie weergeeft.

Rapportages en audits

Om bijvoorbeeld aan te kunnen tonen dat de instelling ‘in control’ is, zou men een uitdraai kunnen maken uit het IdM-systeem, waarmee aangegeven wordt wie toegang heeft tot welke gegevens. Zo’n overzicht kan deel uitmaken van een rapportage aan het management. Bepaal en leg vast wat voor rapportages en audits met welke frequentie voor welke doelgroepen worden opgesteld. Sluit hierbij eventueel aan bij de budgetcyclus.

Kwaliteit

Onder het kwaliteitsbeleid vallen eisen m.b.t. de gebruikte gegevens (volledigheid, correctheid en tijdigheid), eisen m.b.t. de systemen (aanpasbaarheid, bedrijfszekerheid en responstijd) en eventueel eisen aan personeel (welke skills heb je nodig voor welke functie).

Rolmodellen

Rollen worden gebruikt om het bepalen en beheren van autorisaties te vereenvoudigen. Onderdeel van het beleid vormt de beschrijving van de te gebruiken (hoofd-)rollen, zoals Medewerker, Student en Derde. Binnen deze categorieën kunnen diverse subrollen geformuleerd worden. De efficiencywinst die een IdM-project kan inhouden wordt versterkt door het zo veel mogelijk hanteren van dezelfde rolmodellen voor verschillende applicaties, al moet het mogelijk zijn op onderdelen hiervan af te wijken. Dit bevordert de interoperabiliteit, ook over afdelings- en zelfs instellingsgrenzen heen.

Aansluitvoorwaarden

Van een andere orde, maar wel erg belangrijk, zijn de condities waaronder systemen op het IdM-systeem aangesloten kunnen worden. Er zullen beveiligingscriteria geformuleerd moeten worden, opdat aangesloten systemen niet het gehele IdM-systeem kunnen compromitteren. Er moet worden aangegeven welke aansluitwijzen toegestaan zijn (soorten van technische koppelingen, liefst een beperkt aantal), zodat bij de productselectie van doelsystemen daarmee rekening gehouden kan worden. Tenslotte moet een registratie bijgehouden worden van alle aansluitingen, zodat bij onderhoud ook iedereen gewaarschuwd kan worden.

5.4 Relevante wet- en regelgeving

Een van de redenen om het beleid te beschrijven is om aan te tonen dat de instelling voldoet aan relevante wet- en regelgeving.

In het onderwijsveld gaat het altijd over de Wet Bescherming Persoonsgegevens (WBP). De WBP kan vereisen dat gebruikers geïnformeerd zijn over het doel van de registratie van hun gegevens. Indien de gegevens van gebruikers als gevolg van de invoering van IdM maar op één plaats hoeven te worden beheerd, heeft dit voordelen en zal het meestal goed geregeld zijn. Hier is een van de voordelen van IdM direct merkbaar, ook qua kosten.

Voor academische ziekenhuizen is ook de NEN 7510 relevant; hierin worden eisen aan de informatiebeveiliging gesteld. Zeker als het gaat om medische gegevens van personen zullen de vertrouwelijkheid en integriteit van die gegevens goed geregeld moeten zijn. Een degelijk IdM-systeem kan behulpzaam zijn bij het garanderen van de vertrouwelijkheid van persoonsgebonden informatie.

5.5 Tot slot

Het beschrijven en onderhouden van het toegepaste beleid voor IdM-onderdelen zoals identificatie, authenticatie, autorisatie, life cycle management, en dergelijke, is een belangrijk onderdeel van een IdM-project.

Als deze fase correct is uitgevoerd, leidt dat tot de volgende deliverables:

- duiding welke beleidsterreinen onderdeel uitmaken van het IdM-project (en welke niet);
- beschrijving van beleidsuitgangspunten en –randvoorwaarden (voor zover nog nodig);
- bepaling en vastlegging van het beleid voor de diverse IdM-onderdelen;
- beschrijving van relevante wet- en regelgeving en hoe daaraan voldaan wordt.

6. DEELACTIVITEITEN FASE 3: ARCHITECTUUR EN PROCESSEN

De fase 'architectuur en processen' wordt steeds specifiek uitgevoerd voor een bepaald project uit de roadmap. In deze fase kennen we de volgende deelactiviteiten:

1. beschrijving of aanvulling/wijziging van de informatiearchitectuur voor IdM;
2. functionele beschrijving IdM-processen (businesslaag);
3. beschrijving IdM-processen op applicatielaag en datalaag;
4. gap-analyse: bepaling van de wijzigingen van deelactiviteiten 1. t/m 3. t.o.v. de huidige situatie.

6.1 Beschrijving informatiearchitectuur voor IdM-omgeving

De informatiearchitectuur kan worden beschreven door de bij het beleid behorende functionaliteit in IT-termen te vertalen. Daarbij worden de bronnen (personeelssysteem, studenten informatie systeem, systeem voor derden, e.d.) beschreven in relatie tot toepassingen (doelsystemen), zoals intranet, e-mail, agenda, Blackboard, internet, en dergelijke.

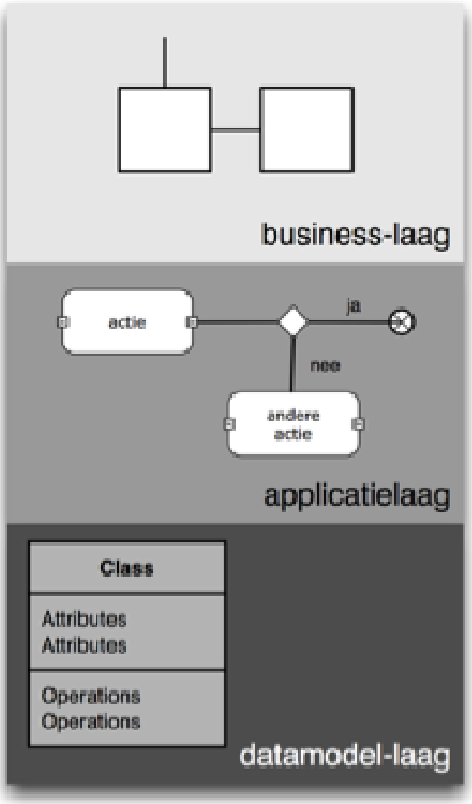
Bepalend voor de informatiearchitectuur is de vraag waar het beheer van identiteitsgegevens van gebruikers is belegd en hoe centraal dan wel decentraal de dienstverlening is georganiseerd. Bij een volledig centraal beheerde ICT-omgeving worden de gegevens van bijvoorbeeld medewerkers centraal in de personeelsadministratie beheerd. In een decentraal beheerde omgeving worden gegevens van bijvoorbeeld externen beheerd door aparte afdelingen, bijvoorbeeld de aanbieder van een laagdrempelige dienst op het intranet. Ook kunnen van een groep gebruikers de meeste gegevens centraal worden beheerd, maar speciale autorisaties decentraal.

We hebben het bij de beschrijving van de informatiearchitectuur in elk geval over de volgende systeemonderdelen:

- bronsystemen voor gebruikers, zoals personeelsregistratiesysteem, studentinformatiesysteem, relatiebeheersysteem, overige gebruikerssystemen;
- doelsystemen, zoals Active Directory, intranet, financieel systeem, helpdesk, mail/agenda, e.d.;
- en daartussen het IdM-systeem, met functies voor (gedelegeerd) beheer, selfservice, zoekfunctionaliteit, personalisatie / authenticatie / autorisatie en tenslotte provisioning (zie ook paragraaf 7.1). Bepaald moet worden wie verantwoordelijk is voor de kenmerken van identiteiten, autorisaties en life cycle management.

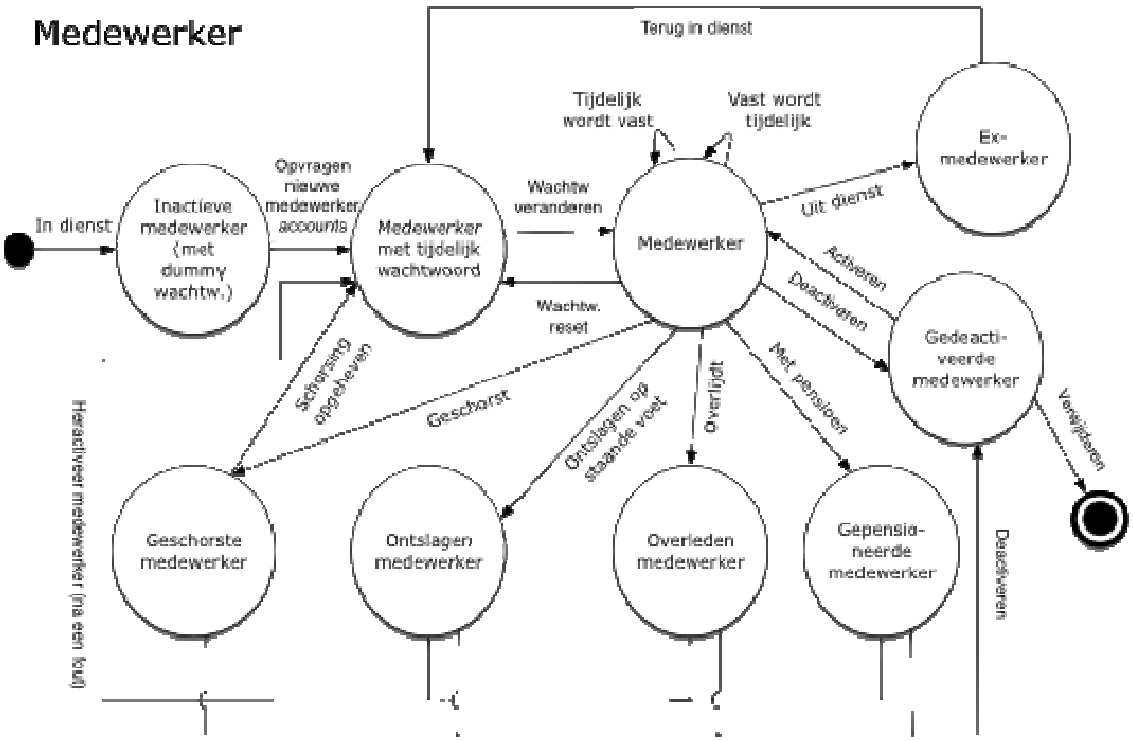
6.2 Functionele beschrijving IdM-processen (businesslaag)

Het meest volledig en overzichtelijk is om een procesarchitectuur op drie lagen vast te leggen. De lagen zijn weergegeven in de onderstaande figuur.



De businesslaag beschrijft de processen in een vorm die de beleidsmakers en proceseigenaren eenvoudig kunnen beoordelen. Denk hierbij aan functionele processen als: 'nieuwe medewerker in dienst', 'medewerker van tijdelijke dienst naar vaste dienst', 'medewerker gaat met pensioen', of: 'scholier wordt student', 'student wordt alumnus', of alumnus overlijdt'. Zo'n functionele beschrijving wordt per doelgroep vaak samengevat in een statusdiagram, waarbij de overgang van de ene status naar de andere een proces vormt.

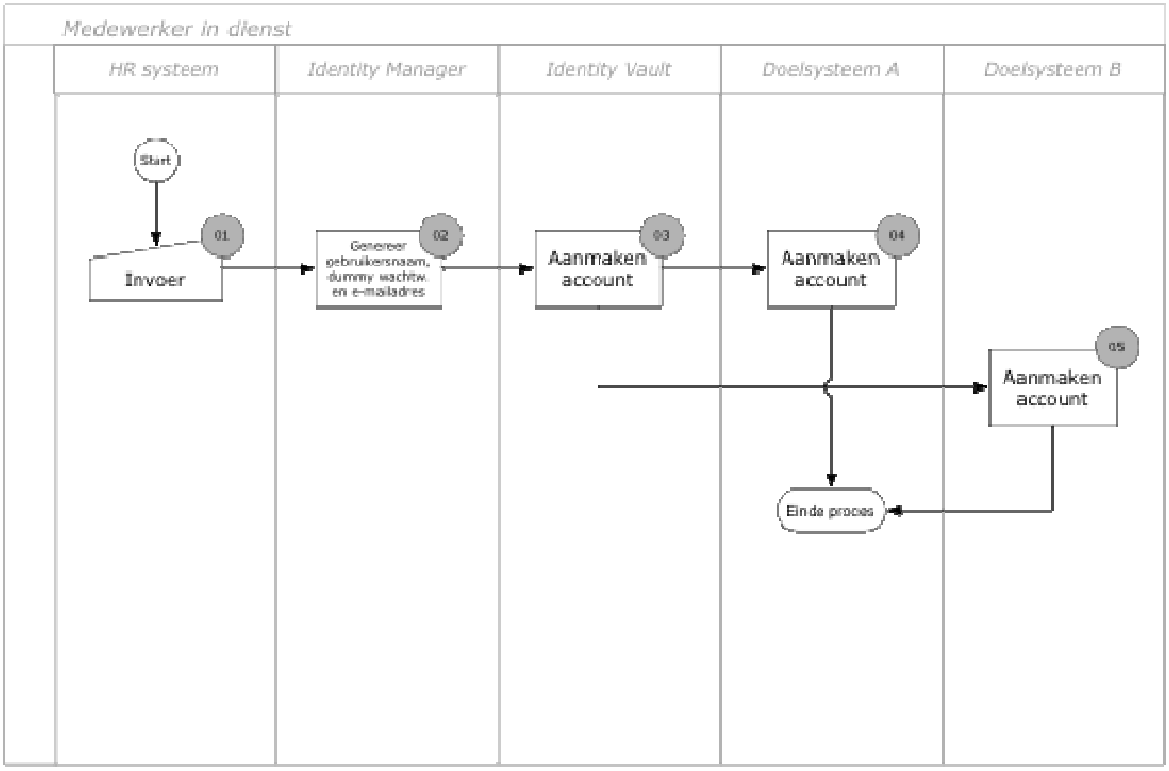
Een voorbeeld van zo'n 'statusdiagram' voor medewerkers:



6.3 Beschrijving IdM-processen

De overige procesbeschrijvingen, die steeds zijn gekoppeld aan de businessprocessen (dus aan een pijltje uit een statusdiagram), zijn vooral bedoeld voor de implementatie en beschrijven welke functies de IdM-applicatie moet bieden en welke data daarbij wordt gebruikt. Denk hierbij bijvoorbeeld aan procesbeschrijvingen als: invoer nieuwe medewerker in HR-systeem, genereer wachtwoord en e-mailadres in de Identity Manager, maak account aan in identity vault en doelsysteem A, etc. Hierbij wordt precies aangegeven welke data uit welke bronnen gebruikt worden en waar deze worden 'weggeschreven'.

De 'vertaling' van een statusdiagram voor medewerkers naar een bijbehorend proces op de applicatielaag kan er voor het proces 'medewerker in dienst' als volgt uitzien:



Op de datalaag wordt aangegeven hoe gegevens uit een bronsysteem afgebeeld kunnen worden op gegevens in een doelsysteem. Bijvoorbeeld: het veld 'Volledige_naam' in een personeelssysteem wordt afgebeeld op 'DisplayName' in Active Directory.

Door de koppeling van de processen en het inrichten van procedures, die zorgen dat bij een wijziging alle beschrijvingen worden aangepast, wordt IdM beter beheersbaar en onderhoudbaar. Dit bevordert de transparantie en maakt compliance op elk moment aantoonbaar.

6.4 Gap-analyse: van huidige naar gewenste situatie

Om de beschreven architectuur en processen te kunnen bereiken, moet geïnventariseerd worden wat de verschillen zijn tussen de huidige en de gewenste situatie. M.a.w. welke aanpassingen zijn noodzakelijk om de nieuwe situatie te bereiken?

Zo'n gap-analyse moet pragmatisch worden aangepakt. Dat de gewenste situatie in voldoende detail beschreven is spreekt voor zich, omdat deze anders niet ingevoerd kan worden. Het is echter niet de bedoeling om de huidige situatie tot in detail te beschrijven, want die moet veranderd worden. Ga voor de huidige situatie uit van de hoofdlijnen en -systemen en vergeet de details, zeker als deze niet terugkeren in de gewenste situatie.

Op basis van de gap-analyse schrijf je een stappenplan voor de gefaseerde doorvoering van de noodzakelijke systeemwijzigingen. Dit stappenplan vormt de basis voor de in fase 4 uit te voeren beschrijving van de technische aanpassingen naar de doelarchitectuur, de definiëring van de (nieuwe) componenten en te hanteren standaarden.

6.5 Tot slot

Fase 3 Architectuur en processen (en ook de vervolgfasen 4 Infrastructuur en 5 Implementatie) wordt steeds doorlopen voor de in de roadmap gedefinieerde deelprojecten, zoals de implementatie van de basisinfrastructuur, de koppeling met Blackboard, of de koppeling met het e-mailsysteem.

De meerwaarde van deze projectfase ligt vooral in de beschrijving van de architectuur en processen op een manier die onderhoudbaar is. Wijzigingen worden gedocumenteerd doorgevoerd, zodat compliance te allen tijde aangetoond kan worden.

Als deze fase correct is uitgevoerd heeft dat de volgende deliverables als resultaat:

- beschrijving informatiearchitectuur voor IdM;
- beschrijving processen op functioneel niveau;
- beschrijving processen op applicatie- en datalaag;
- procedures voor het onderhoud van de procesbeschrijvingen;
- stappenplan noodzakelijke aanpassingen (op basis van gap-analyse).

7. DEELACTIVITEITEN FASE 4: INFRASTRUCTUUR

Ook fase 4 Infrastructuur wordt steeds specifiek voor een bepaald project uit de roadmap doorlopen. In deze fase wordt de functioneel beheerder bijgestaan door de ICT-afdeling, om te garanderen dat de overgang van fase 4 Infrastructuur naar fase 5 Implementatie (volledige verantwoordelijkheid van de ICT-afdeling) soepel verloopt.

In deze fase vinden de volgende deelactiviteiten plaats:

1. Definiëren componenten en standaarden
2. Beschrijven noodzakelijke technische aanpassingen (doelarchitectuur)
3. Keuze van producten en diensten (eventueel)
4. Gap-analyse technische infrastructuur

7.1 Definiëren componenten en standaarden

De 'vertaling' van de informatiearchitectuur, applicaties en data (fase 3) naar te gebruiken technieken (hard- en software) vormt de kern van fase 4.

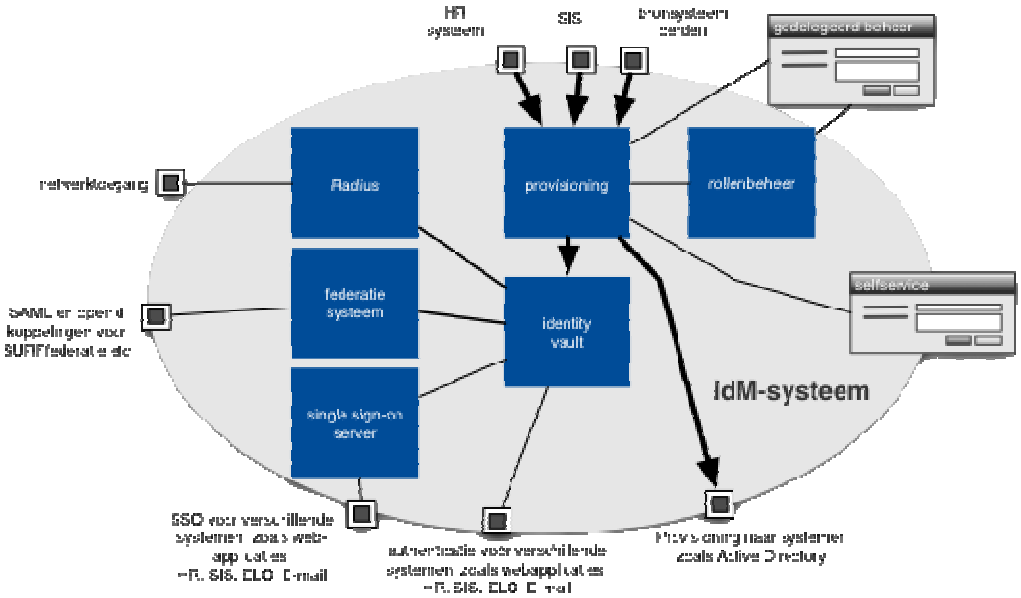
Afhankelijk van de functies die de informatiearchitectuur en de procesbeschrijvingen vragen, komen de volgende componenten in aanmerking:

- systeem voor automatische provisioning en workflows;
- systeem voor rollenbeheer;
- een geconsolideerde database met identiteitsgegevens (vaak 'identity vault' genoemd);
- authenticatiedatabase voor websites (meestal Active Directory of LDAP);
- authenticatiedatabase voor werkplekken (meestal Active Directory);
- authenticatiedatabase voor netwerktoegang (meestal RADIUS);
- systeem voor koppeling aan de SURFfederatie;
- systeem voor single sign-on.

De standaarden die hierbij kunnen worden vastgesteld zijn die voor de interactie van alle systemen met bovengenoemde componenten. Afhankelijk van de strategie kunnen dit bij voorkeur open standaarden zijn en/of die van specifieke leveranciers. Voor provisioning worden meestal meerdere standaarden voor koppeling gekozen, zoals SOAP, databasekoppeling en text based-koppeling, om niet bij voorbaat systemen uit te sluiten van IdM. Het is echter goed om beleid hierover te maken voor nieuw aan te schaffen systemen, waarbij van één of twee opties wordt uitgegaan. Deze kunnen worden meegenomen bij productselecties.

7.2 Beschrijving noodzakelijke technische aanpassingen (doelarchitectuur)

Op basis van de gekozen en beschreven componenten en standaarden wordt de gewenste technische doelarchitectuur bepaald en beschreven. Het geheel vormt de technische infrastructuur. In onderstaande figuur worden de verschillende componenten schematisch weergegeven. Deze figuur kan als uitgangspunt dienen voor het vastleggen van de doelarchitectuur voor een specifieke situatie.



Centraal binnen het IdM systeem staat de identity vault, de geconsolideerde database met identiteitsgegevens. Het IdM-systeem zorgt voor de provisioning van verschillende bronsystemen naar de identity vault. Bronsystemen zijn o.a. de gebruikte HR systemen en het studenteninformatiesysteem. Aan de andere kant worden de gegevens vanuit de identity vault geprovisioned naar de doelsystemen, zoals AD en LDAP.

De provisioning kan plaatsvinden op basis van rollen. Deze rollen moeten dan vastgelegd en beheerd worden in het systeem voor rollenbeheer. De provisioning en het rollenbeheer kunnen beheerd worden m.b.v. een gebruikersinterface. Deze gebruikersinterface is aanpasbaar en zal moeten worden aangepast aan de specifieke eisen en wensen. Naast de gebruikersinterface voor gedelegeerd beheer is er ook nog een "selfservice" gebruikersinterface waarmee gebruikers hunnen eigen account kunnen beheren. Denk daarbij aan het wijzigen van het wachtwoord of het aanvragen van een nieuw wachtwoord.

Naast de identity vault zijn er nog drie systemen die gebruikmaken van de informatie in de identity vault. Een RADIUS-server verzorgt de netwerktoegang. Het federatiesysteem zorgt voor een koppeling met de SURFfederatie en eventueel andere federatieve systemen, De single sign-on server stelt gebruikers in staat met één keer inloggen gebruik te maken van verschillende applicaties.

7.3 Selectie producten en diensten

Indien nodig wordt op basis van de beschreven doelarchitectuur bekeken welke producten daarin een rol moeten spelen.

Bij een productselectie kunnen veel factoren een rol spelen. Deze kwaliteitseisen zijn beschreven in het Extended ISO 9126-model of Quintmodel. In dit model worden zes algemene kwaliteitseisen onderscheiden die elk weer onder te verdelen zijn:

- functionaliteit
  - geschiktheid
  - juistheid
  - koppelbaarheid
  - inschikkelijkheid
  - beveiligbaarheid
- betrouwbaarheid
  - bedrijfszekerheid
  - foutbestendigheid
  - herstelbaarheid
- bruikbaarheid
  - begrijpelijkheid
  - leerbaarheid
  - bedienbaarheid
  - behulpzaamheid
  - gebruikersvriendelijkheid
  - inzichtelijkheid
  - overzichtelijkheid
- efficiëntie
  - tijdsbeslag
  - middelenbeslag
- onderhoudbaarheid
  - analyseerbaarheid
  - wijzigbaarheid
  - stabiliteit
  - testbaarheid

- portabiliteit
  - aanpasbaarheid
  - installeerbaarheid
  - volgzaamheid
  - vervangbaarheid

Deze lijst kan als kapstok dienen om de specifieke eisen te beschrijven waaraan de te selecteren producten aan moeten voldoen. Bij deze beschrijving is het belangrijk dat de beschreven eisen toetsbaar zijn. Op basis van de zo verkregen lijst van eisen kan per product bekeken worden aan welke eisen wel en niet voldaan wordt om zo een weloverwogen keuze te maken.

7.4 Gap-analyse technische infrastructuur

Gap-analyse technische infrastructuur betreft de vergelijking van de huidige situatie met de gewenste situatie. Deze analyse is noodzakelijk om de (technische) koppelingen van bronbestanden en AD, LDAP te kunnen realiseren. Een inproductiename-plan, uitgewerkte migratiescripts en de definitie van de uit te voeren testen ronden deze fase af. In het inproductiename-plan moet aandacht worden besteed aan zaken als fasering (wanneer en in welke volgorde worden verschillende delen van het systeem in productie genomen?) en continuïteit (ondervinden eindgebruikers hinder van de invoering?).

7.5 Tot slot

Fase 4 Infrastructuur is een belangrijke component in de ontwikkeling en implementatie van IdM(-systemen) in een organisatie. Net als fase 3 Architectuur en processen en fase 5 Implementatie, wordt deze fase steeds doorlopen voor de in de IdM-roadmap onderscheiden deelprojecten.

Te vaak wordt de techniek nogal ad hoc aangepakt. Beter is het om dit onderwerp in te bedden in een meer structurele benadering van IdM, die ook daadwerkelijk alle te behalen voordelen realiseert.

De meerwaarde van deze fase ligt in de vertaling van de gewenste architectuur en processen naar benodigde hard- en software.

Als deze fase goed doorlopen is zijn de volgende deliverables beschikbaar:

- beschrijving van de gekozen componenten en standaarden;
- beschrijving van de doel- of systeemarchitectuur;
- keuze van producten en diensten op basis van van te voren geformuleerde eisen en wensen;
- plan van aanpak voor de deelprojecten van implementatie, inclusief migratiescripts en inproductiename-plan.

8. DEELACTIVITEITEN FASE 5: IMPLEMENTATIE

Fase 5 Implementatie wordt steeds specifiek voor een bepaald project uit de roadmap doorlopen. Deze fase is gedeeltelijk het domein van de ICT-afdeling, die de implementatie van het betreffende onderdeel van het IdM-systeem verzorgt.

Deze fase kan worden onderverdeeld in de deelactiviteiten:

1. organisatorische aanpassingen;
2. implementatie basisinfrastructuur;
3. implementatie tactisch niveau;
4. uitvoeren acceptatietests;
5. inproductiename;
6. oplevering IdM-project.

8.1 Organisatorische aanpassingen

De uitvoering van het inproductiename-plan begint met het doorvoeren van de benodigde organisatorische aanpassingen, met als doel de diverse organisatieonderdelen optimaal te laten samenwerken. Dit onderdeel wordt niet door de ICT-afdeling verzorgd, maar door de projectleider in samenwerking met de afdeling Communicatie.

Bedoeling is dat de nagestreefde stroomlijning van definities en procedures bereikt wordt door de gehele organisatie heen. Op deze wijze kunnen de efficiencywinsten optimaal gerealiseerd worden. Falende communicatie kan dit ernstig verstoren.

8.2 Implementatie basisinfrastructuur

De infrastructuur voor IdM wordt doorgaans gefaseerd geïmplementeerd, omdat het te gecompliceerd is om alles in één project goed in te voeren.

Vaak wordt begonnen met de technische implementatie van alle applicaties (de basisinfrastructuur). Vervolgens bepaal je per doelgroep welke systemen je gaat voorzien van ‘intelligentie’, door de bedrijfsregels toe te voegen. Nadat de basisinfrastructuur is aangelegd doorloop je dus per doelgroep en applicatie telkens de paragrafen 8.3 t/m 8.5: toevoegen bedrijfsregels, uitvoeren acceptatietests en inproductiename.

8.3 Implementatie tactisch niveau

Tijdens de daadwerkelijke implementatie moeten de in fase 3 beschreven processen omgezet worden in een verzameling bedrijfsregels die ervoor zorgen dat de life cycle van accounts op de juiste wijze doorlopen wordt. Daarnaast vindt in deze fase de koppeling met de verschillende bron- en doelsystemen plaats. De wijze waarop deze technische implementatie plaatsvindt, is sterk afhankelijk van het geselecteerde product: elk product heeft zijn eigen wijze om de bedrijfsregels en koppelingen vast te leggen. Ook het beheer van rollen en de implementatie van beveiligingsmaatregelen vallen onder de technische implementatie.

8.4 Uitvoeren acceptatietests

Het uitvoeren van acceptatietests dient om te controleren of de implementatie het gewenste resultaat heeft, of dat er nog corrigerende aanpassingen moeten worden doorgevoerd.

Wanneer geconstateerde tekortkomingen verholpen zijn, kan de implementatie op tactisch en technisch niveau afgerond worden.

8.5 Inproductiename

De ingebruikname van het systeem vindt plaats volgens het in de voorgaande fase geschreven inproductiename-plan.

8.6 Oplevering IdM-project

Wanneer geconstateerd is dat het nieuwe of aangepaste IdM-systeem volgens de daaraan gestelde kwaliteitseisen functioneert, moet het project formeel worden opgeleverd / afgesloten. Dat kan door de opdrachtgever een eindrapportage te sturen, waarin verantwoording wordt afgelegd over het gehele traject. Van belang is om over alle aspecten (tijd, geld, kwaliteit, organisatie en communicatie) terug te koppelen of de planning gehaald is en zo niet, welke oorzaken daarvoor zijn opgetreden. Maak duidelijk dat (wellicht ondanks overschrijdingen) het beoogde resultaat gehaald is. Zorg ervoor dat de projectorganisatie ontbonden wordt, nadat het management de leden voor hun inspanning bedankt heeft. Communiceer organisatiebreed dat het project met goed gevolg is afgerond. Voor een nieuw of sterk verbeterd IdM-systeem mag zeker een kick-offbijeenkomst met management en medewerkers georganiseerd worden. Na de officiële startbijeenkomst zal een helpdesk operationeel moeten zijn en kan voor bepaalde medewerkers een trainingssessie behulpzaam zijn.

8.7 Tot slot

Fase 5: Implementatie (en ook de fasen 3 Architectuur & processen en 4 Infrastructuur) wordt steeds doorlopen voor de in de IdM-roadmap gedefinieerde deelprojecten, zoals de implementatie van de basisinfrastructuur, de koppeling met Blackboard, of de koppeling met het e-mailsysteem.

De meerwaarde van deze fase ligt in het realiseren van het IdM-systeem en de oplevering daarvan. Wanneer deze fase gereed is zijn de volgende zaken opgeleverd:

- aangepaste organisatie- en rapportagestructuur;
- implementatie- en beheerrollen en verantwoordelijkheden zijn verdeeld en gecommuniceerd;
- werkend IdM-systeem, inclusief (geautomatiseerde) provisioning;
- eindrapportage van de projectoplevering aan opdrachtgever
- training van beheerders.

BIJLAGE 1: BEGRIPPENLIJST

Account

Een account is het geheel van benodigde gegevens over een gebruiker binnen een applicatie of dienst, zodat deze dienst naar behoren en volgens de wensen van de gebruiker of houder van een informatiesysteem kan werken.

Authenticatie

Bij authenticatie laat de gebruiker zien dat hij beschikt over een authenticatiemiddel dat hoort bij een bepaalde account en identiteit.

De identiteit is vooraf op een andere manier vastgesteld (identificatie). Het doel van de authenticatie is om te laten zien dat gebruiker is wie zij/hij zegt te zijn, maar strikt genomen kan alleen worden vastgesteld dat een gebruiker tijdens de authenticatie het bij een identiteit horende authenticatiemiddel heeft gebruikt.

Authenticatiemiddel

Een voorziening die een gebruiker aanwendt om zich te authenticeren bij een dienst. Voorbeelden zijn een combinatie van een gebruikersnaam en een wachtwoord (zwakke authenticatie), een gebruikersnaam en een certificaat, tokens met wachtwoord (sterke authenticatie).

Autorisatie

Bij autorisatie wordt bepaald waartoe de gebruiker toegang krijgt. Dat kan gebeuren op basis van rollen.

Bedrijfsregels

Regels op beleidsniveau die onder meer bepalen welke personen welke rollen krijgen toebedeeld, welke accounts wanneer in de tijd geldig zijn (life cycle management), hoe gegevens automatisch gegenereerd moeten worden (denk aan e-mailadressen) en welke workflow moet gelden.

Groep of applicatierol

Een rol binnen een applicatie. Deze wordt gegenereerd en toegekend vanuit het IdM-systeem óf binnen een applicatie zelf aangemaakt. In het ideale geval gebeurt dit laatste niet.

Hoofdrol

Rollen kunnen worden vastgelegd in een model. Zo'n model is vaak hiërarchisch. De rollen op het hoogste niveau worden dan 'hoofdrol' genoemd, de overige rollen vaak 'subrollen'. Verder onderscheiden hoofdrollen zich doordat het life cycle management over elk van de hoofdrollen iets moet zeggen. Voor subrollen geldt dat het life cycle management er niet per se iets over hoeft te zeggen. Als dat namelijk niet gebeurt, dan erft een subrol de life cycle managementregels van een hoofdrol.

Identificatie

Het controleren van iemands identiteit aan de hand van persoonsgebonden kenmerken, zoals een paspoort of rijbewijs.

Identiteit

Een identiteit bepaalt één of meer van de volgende zaken:

- wie de gebruiker is (er heeft identificatie plaatsgevonden);
- welke authenticatiemiddelen de gebruiker kan gebruiken;
- of de gebruiker geautoriseerd is voor toegang tot een dienst, liefst d.m.v. rollen;
- welk profiel de gebruiker heeft zodat diensten op maat geleverd kunnen worden.

Een identiteit heeft een uniek kenmerk (unique identifier).

Identity management

IdM is het geheel van processen en techniek voor het beheer en gebruik van elektronische identiteiten.

Identity-managementproces

Het proces of scenario dat wordt gevolgd om accountrechten te verlenen, aan te maken, te verwijderen, enzovoort. Zo'n proces is gebaseerd op de bedrijfsregels. Het proces geeft aan hoe een bedrijfsregel wordt geïmplementeerd, dus welke concrete kenmerken worden gebruikt om een rol toe te kennen, etc.

Let op: in de technische literatuur is vaak sprake van de implementatie van bedrijfsregels in IdM-systemen, waar processen of een deel van processen worden bedoeld.

Life cycle management

Het vaststellen en implementeren wanneer in de tijd de personen die horen bij identiteiten diensten wel of niet mogen gebruiken.

Organisatierol

Een rol die is af te leiden uit de gegevens in de bronsystemen en waarvan de toekenning aan identiteiten ook is af te leiden uit de bronsystemen. Deze rollen reflecteren dus het beeld van de organisatie dat in de bronsystemen bestaat.

Rol

Een rol is een abstracte naam om een functie, plaats in de organisatie, of een taak mee aan te duiden die gebruikt kan worden om – generiek – autorisatie mee te verlenen.

Taakgerichte rol

Een rol die niet is af te leiden uit de gegevens in de bronsystemen en waarvan de toekenning aan identiteiten vaak handmatig moet gebeuren. Ze horen bij een taak die iemand uitvoert, zoals voorzitter van een studentenvereniging, beheerder van het e-mailsysteem, projectmedewerker van project X, lid van de faculteitsraad, etc.

Workflow

Workflow is een gestructureerd IT-bedrijfsproces, waarbij interactie nodig is met sleutelfunctionarissen binnen de organisatie. Denk bijvoorbeeld aan toestemming of controle door een persoon voor het aanmaken van een account.

BIJLAGE 2: VOORBEELDFORMULERING BELEIDSDOELEN IDM

Hieronder volgt een fictief voorbeeld om de toepassing van het zevenstappenmodel voor het formuleren van de juiste beleidsdoelen te verduidelijken.

Situatieschets

Op de universiteit XYZ worden de studenten centraal ingeschreven in het studenteninformatiesysteem. Echter per faculteit heeft het e-mailadres een eigen domeinnaam: studenten Bouwkunde krijgen achter @ eerst BK, en dan de domeinnaam van de universiteit (xyz). Fictief voorbeeld: jan.janssen@bk.xyz.nl. Studenten Scheikunde krijgen eerst SK, fictief voorbeeld: piet.pietersen@sk.xyz.nl. De verschillende faculteiten halen de identiteitsgegevens van een student op uit de centrale studentenadministratie (SIS), maar verzorgen zelf het aanmaken van accounts.

Met hun e-mailadres kunnen studenten inloggen voor bepaalde diensten, die per faculteit kunnen verschillen. Bijvoorbeeld: de bibliotheekcollectie van de faculteit Bouwkunde is alleen toegankelijk voor studenten Bouwkunde; de collectie is afgeschermd voor de studenten Scheikunde.

De faculteiten vinden deze systematiek wel handig. Het geeft ze namelijk ook de gelegenheid om hun systemen zelf in te richten. Zo krijgen bij Bouwkunde personen met de rol 'student' automatisch toegang tot de universiteitsbibliotheken van Parijs en Praag, bij scheikunde tot de bibliotheek van Cambridge. Ook de manier waarop met rollen wordt omgegaan is niet geharmoniseerd tussen faculteiten. De ene geeft een student-assistent een nieuw e-mailaccount met medewerkerbevoegdheden, de andere faculteit doet dat niet. Daarnaast moet een student Bouwkunde drie weken wachten voordat zijn account is aangemaakt, terwijl dit bij Scheikunde één week duurt.

Deze systematiek leidt tot inefficiënties. Aansluiting op de federatie is nog niet gerealiseerd, omdat de aansluitvoorwaarden te strikt zijn.

Bij de centrale afdeling Informatiemanagement is wel duidelijk geworden dat hier een probleem ligt, zowel op het gebied van kostenbeheersing (versnippering is duurder), als op het vlak van gebruiksvriendelijkheid (meerdere malen inloggen) en als gevolg daarvan ook qua beveiliging (teveel wachtwoorden onthouden). Maar het is de vraag of de IT-beheerders bij de afzonderlijke faculteiten daar ook zo over denken.

Tot zover de fictieve situatieschets. Hier is een correcte probleemanalyse noodzakelijk: wat is precies het probleem en wie is de probleemeigenaar? Wat zou Informatiemanagement moeten doen?

Stap 1: Wat is het probleem?

Het huidige IdM-systeem is qua opzet en beheer onvoldoende gestroomlijnd door de gehele universiteitsorganisatie. Definities en beleid worden per faculteit gemaakt, waardoor het systeem te duur is, te gebruiksonvriendelijk en te onveilig. Ook op technisch niveau (architectuur, processen en systemen) zijn er verschillen. De aansluiting op de federatie is hierdoor nog niet gerealiseerd.

Stap 2: Hoe maak je aannemelijk dat dit probleem echt bestaat?

Het aspect van de gebruiksonvriendelijkheid wordt bevestigd door het merendeel van de studenten (én medewerkers!), die regelmatig aanvragen doen voor het resetten van (een van de) wachtwoorden en deze opschrijven om ze niet weer te vergeten. Het aantal aanvragen wordt door de faculteiten bijgehouden; dit is aantoonbaar.

Het veiligheidsaspect is onderbouwd omdat een half jaar geleden een 'mistery man'-onderzoek is gehouden, waaruit duidelijk werd dat medewerkers hun wachtwoord duidelijk zichtbaar hadden opgeschreven.

Het kostenaspect is altijd lastig, zeker in een situatie waarin de kostenmaker er niet altijd voor opdraait. Duidelijk is wel dat er door het ontbreken van een aansluiting op de federatie veel kansen gemist worden en informatie langs andere (duurdere) wegen verkregen moet worden.

Stap 3: Wat wil je met stap 1?

In feite vindt Informatiemanagement de geconstateerde situatie ongewenst, omdat dit de realisatie van de ambities die het College van Bestuur heeft geformuleerd, in de weg staat.

Stap 4: Waarom wil je de situatie veranderen?

De ambities die door het CvB eerder dit jaar zijn geformuleerd luiden:

"De universiteit is een eigentijdse, open organisatie, waarin studenten en medewerkers het beste uit zichzelf kunnen halen, met alle middelen (waaronder informatie) die daarvoor nodig zijn. Het is de ambitie dat de universiteit ook internationaal als een van de beste te boek staat, zowel qua onderwijs als qua research and development."

De geconstateerde situatie met betrekking tot het huidige IdM-systeem staat realisatie van deze ambitie in de weg, omdat vrije informatievergaring en –uitwisseling onvoldoende mogelijk is zonder aansluiting op de federatie.

Stap 5: Wat is de oorzaak van het probleem?

In feite draait het om gebrek aan samenwerking tussen faculteiten. De gedachte dat ICT een 'business enabler' is, mits goed ingezet, leeft kennelijk nog onvoldoende. Goed ingezet betekent in dit geval dat bepaalde voorzieningen geharmoniseerd moeten worden, bijvoorbeeld via een universiteitsbrede 'shared service'. En als dat nog een brug te ver is, dan wel door het harmoniseren van rollen en definities voor IdM tussen faculteiten, waarbij uiteraard de mogelijkheid bestaat om –binnen een bepaalde bandbreedte- eigen oplossingen te implementeren.

Kennelijk is de noodzaak om samen te werken aan stroomlijning van ICT-voorzieningen op faculteitsniveau minder urgent dan op centraal niveau. Zijn de ambities van het CvB wel voldoende uitgedragen?

Stap 6: Welke oorzaken pak je aan?

De (centrale) afdeling Informatiemanagement zou het probleem van de gebrekkige afstemming en samenwerking tussen de faculteiten moeten aanpakken. Het probleem kan onderbouwd worden met de aspecten gebruiksonvriendelijkheid, onveiligheid en het kostenaspect (inefficiënties).

Stap 7: Wat ga je dan concreet doen?

Het lijkt verstandig dat de afdeling Informatiemanagement bij het CvB aankaart dat de huidige (versnipperde) werkwijze m.b.t. IdM de geformuleerde instellingsambities ernstig in de weg staat en dat het ontbreken van een centrale regie daarvan de oorzaak is. Concreet betekent dit dat de afdeling Informatiemanagement een IdM-project zou moeten gaan opzetten, waarin in centraal afspraken gemaakt worden over de doelstellingen van IdM in relatie tot de door de RvC geformuleerde ambities, stroomlijning van beleid en definities, beschrijving van processen en procedures en stroomlijning van werkwijzen.