PvIB Expertbrief – Januari 2011
ISSN 1872-4876, jaargang 7 – Nr. 1

Access management (Deel 2: Architectuur)

Jean-Pierre Vincent

Henk Bel

Ben Elsinga

Wiyaykumar Jharap

Piet Kalverda

Karin van de Kerkhof

Andre Koot

Jan-Roel Löwenthal

Damiën Meijer

Karel van Oort

John van Westeneng

Reviewer:

Renato Kuiper

De laatste jaren zijn vele architectuurmodellen ontwikkeld die het doel hebben weer te geven hoe een optimale identity & access management omgeving moet worden ingericht. De meeste architectuurmodellen bevatten veel dezelfde architectuurcomponenten, en toch zijn ze verschillend.
De vraag die aan deze tweede expertsessie ten grondslag ligt is dan ook of het mogelijk is vanuit de praktijk componenten te beschrijven waarvan we het eens zijn dat ze onderdeel uitmaken van een access management architectuur. Welke zijn dat, in welke mate worden ze toegepast en wat dragen ze bij aan het volwassenheidsniveau van een organisatie?Over componenten met betrekking tot beleid en organisatie (resource management en processen) is de expertgroep het snel eens. Componenten gerelateerd aan informatie, met name het autorisatiemodel, leiden tot meer discussie.

Pagina

2 INLEIDING EN SITUATIESCHETS

Aanleiding

Steeds meer bedrijven buigen zich over identity- en access managementvraagstukken (AM-vraagstukken). Deze vraagstukken zijn in essentie vaak dezelfde, alleen verschillen de bedrijfssituaties en daardoor de oplossingsrichtingen. Om te voorkomen dat 'AM-wielen' opnieuw worden uitgevonden, worden deze vraagstukken door experts geformuleerd en worden aanpak- en oplossingsrichtingen uitgewerkt in 4 expertbrieven, waar deze er een van is. Hierdoor kan de kennis op effectieve wijze worden hergebruikt.

Aanpak

Access management is complex. Het raakt immers alle medewerkers in de hele organisatie op het gebied van logische toegangsbeveiliging. Daarnaast beschikken de meeste bedrijven over een veelvoud aan systemen en een ogenschijnlijk willekeurige combinatie van diverse autorisaties voor medewerkers in deze systemen. Om toch een beeld van access management te kunnen weergeven in expertbrieven, is het onderwerp in vier hoofdgebieden opgesplitst die ieder worden uitgewerkt in een expertbrief. In Bijlage 1 is beschreven hoe deze opsplitsing is uitgevoerd.
Deze expertbrief behandelt deel 2, het onderwerp 'access management architectuur'. In de werkgroep hebben de aanwezige specialisten onderwerpen aangedragen middels een zgn. brownpaper sessie. Deze onderwerpen zijn besproken en verwerkt in deze expertbrief en waar nodig aangevuld en beoordeeld door de betreffende experts.

Scope

De scope van deze expertbrief richt zich op access management. Identity management is buiten scope. Beiden kunnen echter niet zonder elkaar, waardoor het maken van scheiding lastig is. Het is duidelijker om aan te geven dat geen aandacht wordt besteed aan identificatie- en authenticatie-oplossingen, beheer en controle op smart-card-oplossingen, SSO-oplossingen en mechanismes om te controleren of 'je bent wie je zegt dat je bent'. In deze expertbrief gaat de aandacht uit naar wat nodig is voor het verstrekken van autorisaties: beleid, organisatiestructuur, processen, bemensing, administratie en (technische)middelen.

Doelstelling

De expertbrief heeft tot doel een hulpmiddel te zijn bij het implementeren of verbeteren van een access management organisatiestructuur en beheeromgeving. De expertbrief formuleert per onderwerp aandachtspunten waarvan de lezer zelf kan beoordelen of deze in zijn situatie van toepassing zijn en hoe deze in zijn situatie kunnen worden toegepast.

Definitie

Meestal worden identity en access management (IAM) in één adem genoemd omdat deze begrippen sterk aan elkaar zijn gerelateerd. Ter afbakening van het begrip access management, gebruiken we de volgende definities:

Access management is het geheel aan beleid, verantwoordelijkheden, processen en hulpmiddelen dat organisaties in staat stelt om de toegang tot en het gebruik van systemen en informatie te faciliteren, beheren en controleren.

Identity Management is het geheel aan beleid, verantwoordelijkheden, processen en hulpmiddelen dat organisaties in staat stelt om van actoren (als gebruikers en systemen) de identificatie en authenticatie te faciliteren, beheren en controleren.

Toelichting op access management:
Access management betreft het regelen van de toegang van een subject (bijvoorbeeld een medewerker, systeem, service, etc.) tot een object (data of service). In beide gevallen moet worden vastgesteld of het betreffende subject het recht heeft om bij de databron te komen (de resource mag de data inzien of muteren) of de service te gebruiken (bijvoorbeeld: is er een licentie is voor de resource beschikbaar). In een enterpriseomgeving gaat het hierbij om veel rechtenverstrekkingen en de controle daarop (schaalgrootte). Daarom loont het zich om de uitvoering daarvan efficiënt in te richten door middel van helder beleid, strakke processen, juiste bemensing met de bijbehorende verantwoordelijkheden, correcte administraties en goede (technische) hulpmiddelen.

Totstandkoming expertbrief
Deze publicatie is het resultaat van de 2e expertsessie ‘access management’ en is tot stand gekomen met medewerking van de genoemde personen op de voorpagina (zie voor meer achtergrondinformatie bijlage 2).

Initiatiefnemer van de ‘access management’ expertsessies is Jean-Pierre Vincent. Samen met Aaldert Hofman, Bart Bokhorst en Ben Elsinga is de initiële probleemstelling geformuleerd. Deze is verder uitgewerkt door het organisatiecomité.

De organisatiecomitérollen zijn als volgt ingevuld:

Probleemeigenaar:	Karin van de Kerkhof
Facilitator:	Ben Elsinga
Co Facilitator:	Jan-Roel Löwenthal
Ghostwriter:	Jean-Pierre Vincent

4

DE ONDERZOEKSVRAGEN

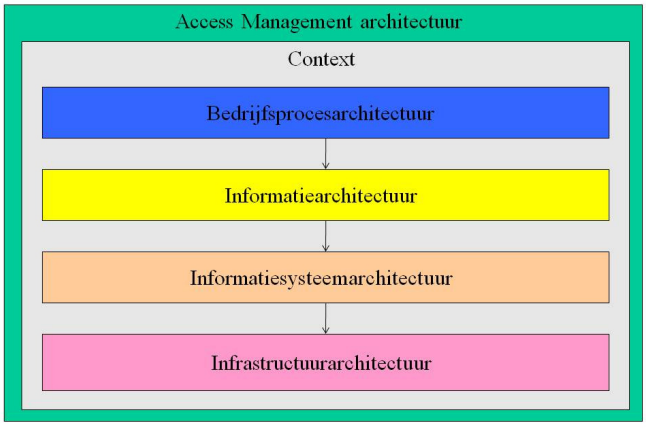
Architectuur: In deze tweede expertbrief wordt access management vanuit architectuur beschreven. Zowel contextueel, als de aspecten omtrent organisatie- en procesinrichting, autorisatiemodellering en techniek.

Probleemstelling voor de expertbrief 'Access Management Architecturen'

Access management experts binnen het PvIB hebben in de loop der tijd vele architectuur ontwerpen voor ogen gehad. De vraag is of deze eenzelfde gedachtegoed op een verschillende manier weergeven of dat er daadwerkelijk verschillende architecturen zijn. Met andere woorden bestaat een access management architectuur in basis uit dezelfde componenten en is er een ideale access management architectuur te definiëren?

N.B. De term 'architectuur' heeft niet voor iedereen dezelfde betekenis. Derhalve wordt hiervoor de definitie uit de expertbrief "security architectuur" (2006) gehanteerd (zie literatuurlijst).

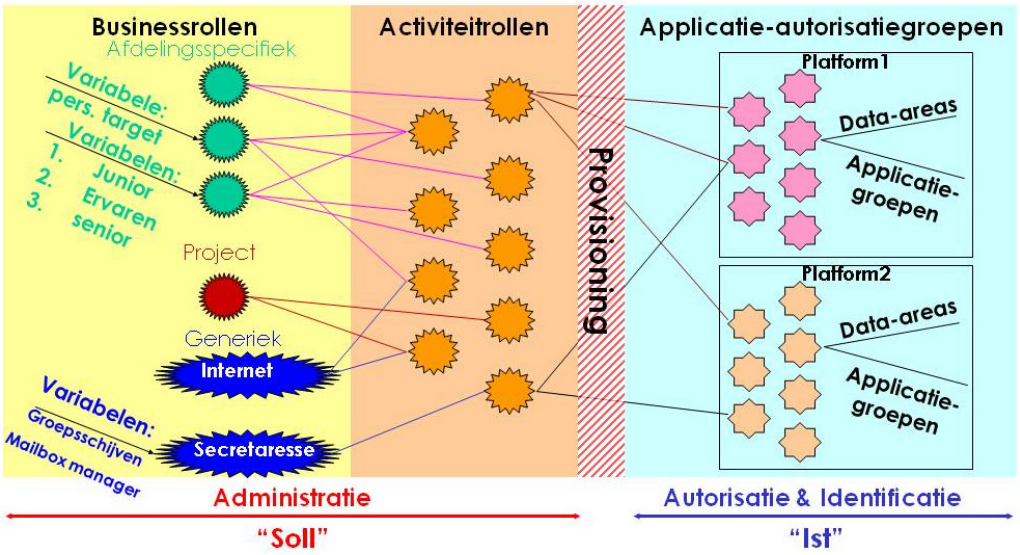
De volgende architectuurlagen worden doorgenomen: Context (beleidsprincipes), de bedrijfsprocesarchitectuur, informatiearchitectuur, informatiesysteemarchitectuur en infrastructuurarchitectuur, zie figuur 1. Van deze architectuurlagen, zal per component in kaart worden gebracht hoe deze is gerelateerd aan de benefits zoals benoemd in de eerste werkgroepsessie.



Figuur 1. AM-architectuur opgebouwd uit deelarchitecturen.

Het onderwerp Context is in de vorm van beleidsprincipes behandeld in expertbrief 1. Een aantal van de meest belangrijke aspecten komt in deze expertbrief nogmaals aan de orde.

Onderdeel van de informatiearchitectuur is het autorisatiemodel, zie een voorbeeld op basis van RBAC in figuur 2. Het autorisatiemodel is fundamenteel voor de hele verdere inrichting van access management in een organisatie. Welke oplossingen kennen we inmiddels en hoe werkbaar zijn die?



Figuur. 2. Voorbeeld van een autorisatiemodel op basis van rollen.

De Informatiesysteemarchitectuur betreft het maken van de keuze voor wel of geen centraal access management systeem en het bepalen hoe deze de access management organisatie faciliteert.

De Infrastructuurarchitectuur betreft onder meer het provisionen van autorisatiegegevens naar en van de doelsystemen.

In de werkgroepsessie is besproken welke componenten in de verscheidene architectuurlagen dienen terug te komen en welke ervaringen en 'lessons learned' we inmiddels kunnen noteren.

Samengevat zijn de uitgangspunten van de sessie de volgende vragen:

1. Bestaat er een ideale architectuur?
2. Wat zijn de belangrijkste architectuurcomponenten en hoe zien deze eruit?
3. Hoe hangen deze componenten samen met de benefits uit de eerste expertbrief (onderdeel businesscase)?
4. Wat zijn de "lessons learned" tav verschillende rollenmodellen (opzet en beheer)?

6 BESTAAT ER EEN IDEAAL ARCHITECTUUR CONCEPT?

Ten aanzien van de vraag of er één ideaal access management architectuurconcept is, zijn de expertsessieleden het over het algemeen eens dat hier hetzelfde antwoord geldt als op de vraag van eerste sessie, is er een ideaal access managementconcept.
Het antwoord is dan ook:
“de aanwezige architectuurcomponenten in een access management omgeving zijn veelal dezelfde, echter zal de wijze van invulling en de diepgang per bedrijfssituatie verschillen. Deze is volledig afhankelijk van migratie van de huidige situatie naar de nagestreefde oplossing en daarmee van het gewenste volwassenheidsniveau van de organisatie.”

Deze expertbrief beschrijft daarom niet een ideale architectuur met ideale componenten. Wel worden architectuurlagen en belangrijke componenten beschreven. Deze zijn bedoeld als handvat bij het maken van de juiste overwegingen over na te streven oplossingen.

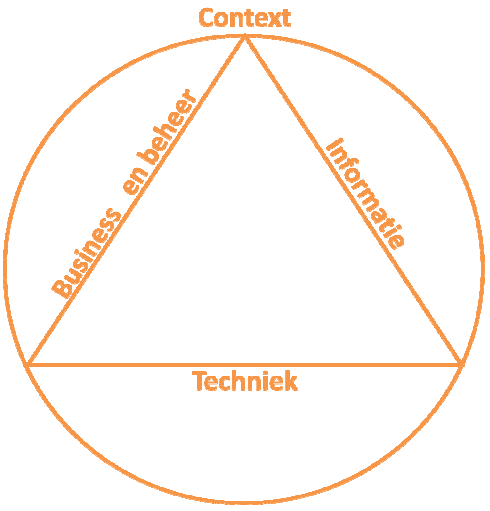
Het is beter te stellen dat het goed mogelijk is om per component een referentieconcept te beschrijven, die informatie en/of mogelijke oplossingen aanreikt om te worden hergebruikt.

ARCHITECTUURLAGEN

Dit hoofdstuk gaat in op de access management architectuur opzet. Aspecten daarbij zijn:
- Architectuurlagen;
- Architectuurcomponenten;
- Structuur (gestandaardiseerd/gecentraliseerd);
- Relatie tussen autorisatie en identiteit;
- Controleerbaarheid en controlevorm.

In de probleemstelling is een voorbeeld van een architectuurlagenmodel opgenomen. Tijdens de sessie benoemen we de Bedrijfsprocesarchitectuurlaag echter specifieker. We gaan in op de organisatiestructuur, actoren en processen, gezien zowel vanuit een business- als een beheer (IT) –perspectief. De informatielaag is voor access management de meest belangrijke laag. De uitwerking van deze laag bepaalt:
- Hoe wordt voldaan aan beleid.
- Hoe gebruikersvriendelijkheid voor de business wordt verkregen.
- Hoe groot de beheerinspanning zal worden.

Verder wordt in de probleemstelling informatiesystemen en infrastructuur als twee lagen aangegeven. In de expertbrief zijn die twee lagen samen genomen onder de term technische architectuurlaag.
Het geheel wordt hier ook omsloten door de context. Onderstaande figuur geeft deze lagen gevisualiseerd weer.



Figuur 3. De drie architectuurlagen omsloten door de context.

8

Access managementomgeving architectuur opzet

Een access management omgeving kent 2 hoofdvormen. In de huidige praktijk is de standaardsituatie dat het access management landschap uit losse eilandjes bestaat met allerlei formele en informele onderlinge relaties. De streefarchitectuur is vaak een vorm waarin processen en tooling zijn gestandaardiseerd. Wanneer verbeteringen worden nagestreefd is een eerste beleidskeuze dan ook in hoeverre centralisatie van autorisatie-administraties en autorisatiebeheerprocessen wenselijk is. Een reden om te kiezen voor centralisatie kan zijn dat de kosten dan over het algemeen lager zijn.

Uiteindelijk faciliteert een access management omgeving alleen dat via afgesproken processen en verantwoordelijkheden mutaties worden aangebracht in autorisatie-administraties. Het gaat er daarbij wel om dat deze flexibel, inzichtelijk en controleerbaar zijn.

De mate van ‘in control’ zijn

Een belangrijk aspect voor de opzet van de architectuur is in welke mate de relatie tussen een autorisatie en de identiteit van de gebruiker moet zijn vastgelegd. Rechten kunnen worden gekoppeld aan identiteiten, maar rechten kunnen ook worden gekoppeld aan de context van identiteiten. Bijvoorbeeld alle accountmanagers mogen in het klantenbestand kijken. In dat geval kan de autorisatie op basis van de context van de identiteit worden vastgesteld, namelijk of de betreffende gebruiker een accountmanager is. Wanneer dergelijke toegangsmechanismes worden toegepast, moeten ook de contextgegevens beschikbaar en betrouwbaar zijn.

Een ander belangrijk aspect voor de opzet van de architectuur is de gestelde eis aan de mate van controleerbaarheid. Zoals ook in expertbrief 1 is aangegeven, is de bedrijfscultuur/omgeving een hoofdfactor. Een relatief open omgeving (zoals een ziekenhuis) zal een architectuur kiezen die meer is gebaseerd op controle achteraf. Een relatief gesloten omgeving (financiële instelling) wil op voorhand voorkomen dat fraudegevoelige situaties kunnen ontstaan. Het vaststellen van de mate van openheid of geslotenheid is essentieel voor het vaststellen van een optimale architectuur en daarmee de keuze voor de architectuurcomponenten.

ARCHITECTUUR COMPONENTEN

Architectuurlagen bevatten architectuurcomponenten. Deze componenten beschrijven onderwerpen die van toepassing zijn in de betreffende laag. Alle in dit hoofdstuk beschreven onderwerpen, zijn in meer en mindere mate van toepassing in een access management omgeving. Voor het efficiënt inrichten/verbeteren van deze omgeving moet per component worden bepaald hoe de organisatie er nu voor staat, hoe 'zwaar' het onderwerp moet worden gewogen en hoe deze moet worden ingevuld. Mede bepalend voor de weging en invulling zijn criteria als businessdrivers en compliancy-eisen. Deze worden in het volgend hoofdstuk behandeld.

Alle architectuurcomponenten hebben een life-cycle. Iedere component wordt ontwikkeld, beheerd en weer afgebouwd. Het life-cyclemanagement van componenten vindt plaats middels processen en resources met specifieke taken & verantwoordelijkheden. Per component moet het life-cyclemanagement in een access management omgeving worden ingeregeld.

Contextuele componenten (visie en beleid)

Het uitwerken van een architectuur begint met het vaststellen van de context (bedrijfsprincipes en het bedrijfsbeleid). Bedrijfsbeleid is bepalend voor de wijze waarop de componenten in de onderliggende architectuurlagen worden uitgewerkt.

De 1e expertbrief over Access Management beschrijft uitgebreid de beleidsonderwerpen die aan de orde zijn in deze architectuurlaag. Vanwege de topdown benadering door de verschillende architectuurlagen in deze expertbrief, komt een aantal nieuwe beleidsonderwerpen aan de orde.

In onderstaande tabel worden contextuele componenten, producten of onderwerpen (CC) genoemd. De tabelregels zijn uniek genummerd om verderop in de expertbrief verbanden te kunnen leggen tussen tabelregels uit de andere tabellen.

Nr	Component, product, onderwerp	Omschrijving
CC1	Taak- en verantwoordelijkheids-principes	Een belangrijk inrichtingsprincipe voor access management is dat iedere component een eigenaar heeft. Deze is verantwoordelijk voor de wijze van uitvoering en derhalve ook voor de toepassing van het beleid. Vanuit beleid kunnen bijvoorbeeld eisen worden gesteld aan de workflow in een component. Aanvragen voor gevoelige autorisaties zouden bijvoorbeeld altijd aan een extra controle of goedkeuring moeten worden onderworpen. Dat betekent dat de workflow afhankelijk wordt van extra gegevens. Die extra gegevens dienen dan ook beschikbaar te zijn. In dit geval spreken we bijvoorbeeld over het classificeren van autorisaties.
CC2	Goedkeuringsprincipes	Het beleid moet voorschrijven wie beslist of autorisaties

		wel of niet worden verstrekt. Bij een sterk business-gedreven en open organisatie, waar weinig echte gevoelige gegevens aanwezig zijn, kan deze taak volledig bij de aanvrager worden belegd. Als de aanvrager het wil, dan krijgt hij dat. Waarschijnlijk zal in zo'n situatie veel aandacht zijn voor het aanwezig zijn van loggings, zodat kan worden nagegaan wie wat heeft gedaan en altijd kan worden onderzocht waarom. In fraudegevoelige om-gevingen zal deze taak expliciet zijn belegd bij een data-eigenaar en of security-officer. Deze bepaalt dan of een aanvrager de aangevraagde autorisatie wel of niet krijgt.
CC3	Delegatieprincipes	Een inrichtingsprincipe is dat het beheer moet worden opgedeeld in afzonderlijke componenten en wel zodanig dat ze te delegeren zijn of elders onder te brengen zijn. Bijvoorbeeld een manager die het aanvragen van autorisaties uitbesteed aan een medewerker op de afdeling of vanuit een centraal orgaan naar decentrale uitvoeringseenheden. Naar de omgeving toe werken deze gelijk, via beleidsprocessen en/of gecentraliseerde of uniforme autorisatieprocessen.
CC4	Beleid	Beleidsregels moeten zodanig concreet zijn, dat ze als basis kunnen worden gebruikt voor het maken van rules en procuratierichtlijnen.
CC5	Accounting	Beleidsregels moeten aangeven in hoeverre controles moeten worden uitgevoerd. Moeten bijvoorbeeld handelingen altijd terug te voeren zijn naar de persoon? In dat geval zijn systeemaccounts ongewenst of moeten oplossingen worden bedacht om tussen systemen identificatie-gegevens uit te wisselen. Ook kunnen access management (bescheiden) doelstellingen in KPI's van managers worden opgenomen om hen bewust te maken welke verantwoordelijkheid zij hebben met betrekking tot access management.
CC6	Auditrichtlijnen	Beschreven moet worden welke eisen worden gesteld aan access management auditprocessen; bijvoorbeeld hoe vaak moeten bepaalde audits worden uitgevoerd en hoe zwaar zijn de sancties. Het meest bekende auditproces is het uitvoeren van een Soll-Ist vergelijking (welke autorisaties zou een medewerker moeten hebben en welke heeft hij daadwerkelijk). Maar andere vormen van Soll-Ist vergelijkingen zijn ook mogelijk, bijvoorbeeld welke medewerkers zouden dezelfde autorisaties moeten hebben of worden access management beleidregels daadwerkelijk toegepast zoals ze zijn bedoelt, etc..
CC7	Functiescheidingsbeleid	Beleidsregels moeten aangeven hoe met functiescheiding dient te worden omgegaan en wie beslist hoe uitzonderingssituaties worden uitgewerkt.

Business- en beheer-componenten

Dit onderdeel betreft de organisatorische structuur, processen en resources die de dagelijkse uitvoering van access management mogelijk maakt. De businesscomponenten (CB) bestaan voornamelijk uit het benoemen van taken & verantwoordelijkheden en het beschrijven van processen aan de kant van de business. Voor de beheercomponenten geldt hetzelfde aan de kant van IT met de toevoeging dat de access management organisatiestructuur hier ook onderdeel van uitmaakt.

In onderstaande tabel staan de besproken componenten weergegeven. Opvallend was dat in de sessie de term ‘proces’ en ‘workflow’ veelvuldig door elkaar werd gebruikt. Het beeld is dat workflows onderdeel zijn van een proces.

Nr	Component, product, onderwerp	Omschrijving
CB1	SLA’s	Access management SLA’s bevatten de afspraken omtrent de autorisatieafhandeling tussen verschillende partijen die onderdeel uitmaken van de access management omgeving. De kaders voor de SLA’s worden o.a. gesteld door business wensen en beleidscomponenten. Zo worden bijvoorbeeld performance eisen (hoe snel een aanvraag wordt afgehandeld) gesteld vanuit de business, maar bijvoorbeeld risk/security management stelt eisen aan de medewerking van de business bij het uitvoeren van audits.
CB2	Procescomponenten	Procescomponenten zorgen ervoor dat een startsituatie naar een eindsituatie wordt gebracht. Medewerkers voeren met behulp van middelen aaneensluitende activiteiten uit conform de beschreven processencomponenten. De procescomponenten bestaan uit de volgende logische taken: aanvragen, registreren, interpreteren, uitvoeren, controleren, fiatteren en terugkoppelen. Dat deze taken kunnen worden uitgevoerd is de verantwoordelijkheid van de proceseigenaar. Bij het uitvoeren kunnen derden zijn betrokken. Met deze partijen moeten afspraken zijn/kunnen worden gemaakt. Vastgelegd moet zijn: wie bepaald wat wel en niet mag.
CB3	Procescomponent instroom	Dit betreft de eerste stap in het medewerkerlifecycle-management. Wanneer een medewerker in dienst komt moet deze worden voorzien van autorisaties. Dat betekent dat het HR-proces, dat hieraan voorafgaat, moet aansluiten op een autorisatie-verstrekkingsproces. Het HR-proces voorziet meestal in het definiëren van de unieke identiteit en identiteitgegevens (als het toekennen van personeelsnummer, HR-functie, afdeling, etc.). Vragen die van toepassing zijn in het autorisatie verstrekkingproces zijn: welke autorisaties kunnen automatisch worden toegekend en welke dienen door de manager te worden aangevraagd. Belangrijk punt daarbij is de snelheid waarmee de autorisaties kunnen worden verstrekt.
CB4	Procescomponent	Dit betreft de tweede stap in het medewerkerlifecycle-

	doorstroom	management. Wanneer een medewerker doorstroomt naar een nieuwe functie op een andere afdeling, moeten de oude autorisatie worden ingetrokken en nieuwe worden verstrekt. Daarbij moet worden geregeld dat alleen de verschillen tussen de aan te brengen en in te trekken autorisaties daadwerkelijk in de doelsystemen worden aangepast om te voorkomen dat eerst autorisaties worden ingetrokken die later weer worden verstrekt. Bij een doorstroming moet het mogelijk zijn een overbruggingsperiode te hanteren waarbij zowel de oude als de nieuwe autorisaties actief moeten blijven. Vastgesteld moet zijn welke manager van de medewerker verantwoordelijk is voor de 'dubbele' situatie en hoe wordt geregeld dat na de overbruggingsperiode ook daadwerkelijk de oude autorisaties worden ingetrokken.
CB5	Procescomponent uitstroom	Dit betreft de laatste stap in het medewerkerlifecycle-management. Wanneer een medewerker de organisatie verlaat moeten na de laatste werkdag alle autorisaties worden geblokkeerd of ingetrokken. Van belang is te bepalen wie daarvoor verantwoordelijk is, de manager of HR en welke administratie het intrekken van de autorisaties regelt (HR- of een centrale autorisatieadministratie). Een praktische ervaring is dat met bijvoorbeeld externen inhuur de verlenging van een contract pas op het laatste moment geschied en de HR-administratie niet tijdig wordt bijgewerkt. Het verdiend daarom de aanbeveling om bij een geautomatiseerd proces, de betreffende accounts en autorisaties eerst te laten blokkeren en pas na een periode van bijvoorbeeld een week, daadwerkelijk te laten intrekken. De manager van de medewerker zit hierbij aan het stuur. In de AM-administratie moet de relatie tussen het unieke medewerker-ID en de accounts goed zijn vastgelegd
CB6	Procescomponent audit	Goed ingericht Identity & Access Management helpt bij het 'in control' zijn. Dit kan inzichtelijk worden gemaakt met goede audit processen en rapportages. Zeker wanneer met een centrale autorisatieregistratie wordt gewerkt en automatic provisioning is ingericht, kunnen eenvoudig volledige rapportages worden gegenereerd. De rapportages moeten inzicht kunnen geven in belegd eigenaarschap, Soll-Ist vergelijkingen van verstrekte autorisaties en user-id's. Bijvoorbeeld: zijn de juiste autorisaties verstrekt, zijn die conform beleid en zijn er alleen userd-id's actief van medewerkers die in dienst zijn.
CB7	Procescomponent doorbelasting	Een autorisatieadministratie kan voor sommige systemen worden gebruikt om IT-kosten door te belasten aan de business. Bijvoorbeeld als het gaat om userlicenties of als de beheerkosten te vertalen zijn naar autorisaties.
CB8	Procescomponent	Het beleggen van het callafhandelingsproces bij de

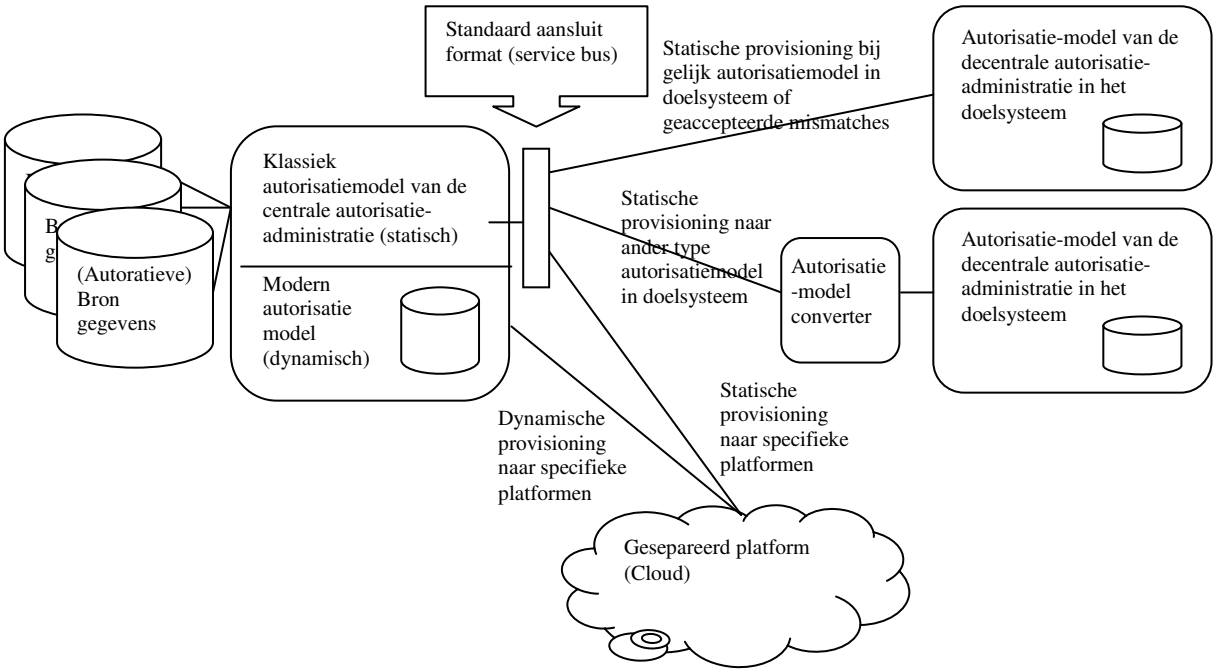
	incident management	servicedesk, 2e en 3e lijn is complex. De betreffende partijen moeten goed bekend worden gemaakt met het toegepaste autorisatiemodel, hoe deze is ingevuld en wie daarin beslissend zijn. Gezien de grote hoeveelheid informatie en de praktijkervaringen die nodig zijn om voldoende inzicht te hebben in de problematiek, is het zeer aan te bevelen deze partijen intensief te betrekken bij het uitrollen van access management. Daarnaast moeten deze partijen inzicht hebben in de boven genoemde gegevens.
CB9	Autorisatiemodel life-cycle management	Dit betreft het aanmaken, muteren en verwijderen van rollen, rules en/of andere autorisatiemodelcomponenten. Dit gebeurt, als het goed is, alleen bij wijzigingen van of in de betreffende werkomgeving. Voor goed life-cycle management is het van belang het eigenaarschap goed te beleggen en eigenaren bewust te houden van hun taken en verantwoordelijkheden.
CB10	Procescomponent innovatie Ontwerpen applicaties/ systemen	Wanneer een nieuw systeem wordt ontwikkeld of aangeschaft, moet deze worden aangesloten op het autorisatiemodel. Dit systeem moet daarom voldoen aan eisen die het centrale autorisatiemodel met zich meebrengt. Als dat niet lukt moet in de ontwikkeling/ aanschaf een aansluitmodel worden ontwikkeld. Een aansluitmodel kan een handmatig proces zijn of een geautomatiseerd proces. Deze uitkomst wordt meestal bepaald door de achterliggende businesscase.
CB11	Procescomponent innovatie (projecten, change management)	Projecten voeren doorgaans wijzigingen in de werkomgeving door. Dat kunnen bijvoorbeeld reorganisatieprojecten zijn of uitrolprojecten van nieuwe systemen. Bij dergelijke projecten zijn altijd wel autorisatiemutaties aan de orde Bij de implementatie (uitrol) moet het project daarom worden voorzien van gebruikers- en autorisatieinformatie (wie zijn doelgroepen, waarom hebben die de huidige autorisaties, etc.) en van uitrolaanpak-informatie, bijvoorbeeld: hoe regel ik een gedoseerde uitrol, hoe voorkom ik bigbang problemen, hoe regel ik roll-back.
CB12	Delegatie	De Access Management architectuur moet voorzien in het kunnen delegeren van taken. Bijvoorbeeld het aanvragen van autorisaties wordt vaak voorbereid door inhoudelijke kundige medewerkers. De manager van de medewerker zet dan de aanvraag door. Een autorisatie- of data-eigenaar moet dan de aanvraag kunnen goedkeuren en doorzetten naar een autorisatiebeheerder . Zowel voor de manager als de autorisatie- of data-eigenaar geldt dat deze hun taken moeten kunnen delegeren of uitbesteden (bijvoorbeeld bij ziekte of vakantie). Het delegatieproces met de bijbehorende administratie, moet worden ondersteund door goede tooling.
CB13	RACI	Het benoemen van de taken & verantwoordelijkheden is cruciaal voor goed access management. Dit geldt met

		name voor het benoemen en beleggen van de taken: eigenaar (roleigenaar, rule-eigenaar, autorisatie-eigenaar, data-eigenaar), manager, fiatteur, controleur (auditor), autorisatiemodelontwerper en autorisatiebeheerder. Hierbij moeten functiescheidingsregels worden toegepast.
CB14	Policy Decision Point (PDP)	Op grond van vastgestelde criteria en toegewezen taken en verantwoordelijkheden, beslissen wat de gebruiker wel en niet mag.
CB15	Policy Enforcement Point (PEP)	Betreft het verstrekken van de toegang zoals die bij het policy decision point is vastgesteld.
CB16	Rolemining component	Rolemining kan worden toegepast voor het genereren van rollen. Hierbij wordt geanalyseerd welke autorisaties aan dezelfde (soort) medewerkers zijn toegekend. De methode wordt overigens ten sterkste afgeraden omdat het betekenisloze rollen oplevert. De autorisaties in deze rollen hebben geen directe samenhang en er wordt ook geen antwoord gegeven op de vraag waarom de te koppelen medewerkers over de betreffende autorisaties beschikken. Het gevolg is dat het beheer van deze rollen complex, duur en traag wordt. De methode is wel richtinggevend als deze binnen een beperkte scope wordt toegepast, bijvoorbeeld per primair bedrijfsproces, zie CI5 op blz. 18.
CB17	Rulemining component	Rules kunnen onder andere worden afgeleid uit (concrete) beleidsregels. Hoe dit dient te geschieden en hoe het beheer wordt belegd wordt in deze component bepaald. Ook hier geldt dat het de aanbeveling verdient dat rules logisch uit te leggen moeten zijn en niet alleen een feitelijke constatering. De ervaring leert dat rules goed kunnen worden toegepast op autorisaties die aan grote groepen medewerkers worden toegekend. Hoe specifieker hoe lastiger de rule. Voor specifieke autorisaties is het in de meeste gevallen eenvoudiger andere toekenning-methoden toe te passen, bijvoorbeeld middels losse aanvragen of RBAC. Rules kunnen worden toegepast op medewerker-autorisatierelatie, maar ook op bijvoorbeeld medewerker-rol relatie. De combinatie van rollen met rules wordt steeds vaker gebruikt (ook wel RRBAC genoemd).
CB18	Gegevensbronnen	Belangrijk is dat goed wordt onderzocht wat de kwaliteit van de gegevensbronnen is die de processen ondersteunen. De betreffende gegevensbronnen die de AM-processen voorzien van informatie zijn daardoor verheven tot autoratieve bronnen, waarvoor ook de daaraan gestelde eisen van toepassing zijn. Zie ‘Informatiecomponenten’.

Informatiecomponenten

Onder informatie verstaan we alle gegevens die worden gebruikt in de access management omgeving. Dat betreft gegevens over gebruikte doelsystemen, de autorisaties in die systemen, goedkeuringen en identiteitgegevens (autoratieve bron). Omdat de expertbrief gaat over access management en niet over identity management is de aandacht voor identiteitgegevens beperkt tot op hoofdlijnen.

Het invulling geven aan informatiecomponenten (IC) is sterk afhankelijk van het wel of niet centraal opslaan van autorisatie-informatie (informatie over autorisaties en aan te brengen wijzigingen). In deze expertbrief wordt in principe uitgegaan van een autorisatie-informatiestructuur zoals in figuur 4 weergegeven. De structuur betreft hier een centrale administratie die de basis vormt voor de uitgegeven autorisaties in de doelsystemen. Deze kan uit twee delen bestaan statisch en dynamisch (zie toelichting CI1 en LL7). Eventuele afwijkende modellen in de doelsystemen worden via ‘convertors/adapters’ aangesloten op de centrale administratie.



Figuur 4. De koppeling tussen een centraal autorisatiemodel en decentrale autorisatiemodellen.

16

In onderstaande tabel worden informatiecomponenten beschreven. In CI5 tot en met CI9 zijn verschillende typen autorisatiemodellen beschreven.

Nr	Component, product, onderwerp	Omschrijving
CI1	Autorisatiemodellen	Een autorisatiemodel is de wijze waarop een toegangsadministratie is georganiseerd. We onderkennen twee toepassingen van autorisatiemodellen, in een doelsysteem (Ist) en als (centrale) autorisatieadministratie (Soll). Ieder doelsysteem beschikt over een eigen autorisatiemodel. Een autorisatiemodel in een doelsysteem kent meestal één structuur of methode. Autorisatiemodellen van doelsystemen verschillen onderling meestal. Dit komt of doordat verschillende methoden worden gebruikt of omdat verschillende visies op dezelfde methoden zijn toegepast. Een autorisatiestructuur van een centrale Soll-administratie kan zijn opgebouwd uit meerdere autorisatiemodellen. Principes en beleidskeuzes (zie expertbrief 1) zijn sterk van invloed op de te kiezen combinatie van modellen, bijvoorbeeld: hoe moet worden omgegaan met need to know, broadempowerment, dure userlicenties, etc. Via het centrale administratiemodel worden soms ook zaken als printertoegang geregeld. Een goed autorisatiemodel zou ook kunnen voorzien in het toekennen van middelen als een laptop of leaseauto door toegang tot de bestelsystemen te verschaffen. Steeds vaker worden ook ‘niet’ IT-aspecten geïntegreerd met access management zoals bijvoorbeeld asset managment en fysieke-toegang. Een essentiële vraag voor het ontwerpen van een centraal autorisatiemodel is: op basis van welke criteria bepaalt een doelsysteem welke toegang wordt verleend bij een gebruikersactiviteit. Wordt, wanneer een gebruiker zich aanmeldt bij een doelsysteem, vastgesteld of hij toegang krijgt op basis van zijn identiteit (zijn id) of op basis van identiteitscriteria (eigenschappen van de identiteit). Een voorbeeld van een criterium toekenning is: in het doelsysteem is geadministreerd dat accountmanagers klantgegevens mogen lezen. Wil een accountmanager de gegevens lezen dan checkt het doelsysteem niet op het id van de accountmanager, maar op het criterium of de

		medewerker accountmanager is. Deze vraag is essentieel, omdat het bepaalt welke gegevens op welk moment in het autorisatieproces beschikbaar dienen te zijn. Kan een doelsysteem op het moment van de gebruikersactiviteit bepalen of het een geoorloofde gebruikersactiviteit is (op dat moment worden gegevens uitgewisseld en gewogen), of moeten de gegevens op voorhand in de doeladministratieaanwezig zijn. Het bepaalt ook of eenmalig een autorisatie in een doelsysteem wordt verstrekt (statisch) of dat de autorisatie bij iedere gebruikershandeling wordt verstrekt (dynamisch). Een vorm van statische autorisatievaststelling is het opslaan van het user-id van de accountmanager in het doelsysteem met de daarbij behorende autorisatie- en authenticatiegegevens (bijvoorbeeld een wachtwoordhash). Dit is de meest gebruikte vorm, met name in legacy systemen. In SOA-omgevingen wordt steeds meer dynamische autorisatie toegepast.
CI2	Autorisatiemodelkoppeling	Wanneer een centrale autorisatie-administratie (Soll) wordt aangelegd, moet deze kunnen worden gekoppeld aan de administraties in de doelsystemen (Ist). Idealiter zijn de autorisatiemodellen van beide administraties gelijk, maar in de praktijk is dat vrijwel nooit het geval. Ieder doelsysteem heeft een eigen autorisatiestructuur. Een directe koppeling kan derhalve mismatches opleveren. Wanneer de centrale administratie en een doelsysteemadministratie beide zijn opgebouwd uit rollen (RBAC), kan de rol (vaak profiel genaamd) in het doelsysteem bijvoorbeeld ruimere autorisaties bevatten dan voor de rol in de centrale administratie strikt noodzakelijk is. Vooral voor bijvoorbeeld legacy-systemen is de businesscase om het autorisatiemodel om te zetten vaak niet positief. Mismatches zijn overigens ook lang niet altijd erg, zolang deze maar weloverwogen geanalyseerd worden. Soms maken specifieke platformen onderdeel uit van de IT-omgeving. Een specifiek platform heeft vaak ook een eigen specifiek autorisatiemodel. Als het een cloud betreft kunnen in sommige gevallen hierover afspraken worden gemaakt. Sommige platformomgevingen hebben een eigen autorisatiebeheeromgeving en/of aanvullende autorisatieprocessen. Met deze omgevingen moeten heldere afspraken worden gemaakt over het aanleveren

		van (autorisatie-) gegevens vanuit de centrale beheeromgeving, middels SLA-afspraken (ook over beschikbaarheid, toegankelijkheid, etc.) met de business en over het aanleveren van autorisatieinformatie, bijvoorbeeld m.b.t. audits. Cloud-omgevingen zouden, vanuit logisch niveau gezien, de bij iedere inlogactie van een gebruiker de autorisatiegegevens uit de centrale administratie moeten halen (dynamisch). Praktisch en technisch gezien kunnen clouds bijvoorbeeld een windows-omgeving, mainframe-, SAP-, etc.-omgevingen zijn. Binnen de clouds worden op een eigen manier autorisatiegegevens doorgegeven. Ze zouden niet zelf een autorisatie administratie moeten bevatten, anders dan bijv. logginggegevens. Helaas werkt dit tegenwoordig meestal nog niet zo. Voor de communicatie tussen de clouds moet worden vastgesteld welke (standaard of specifieke) protocollen worden toegepast, zie: 'Technische componenten'.
CI3	Autorisatiemodelconverter	Een autorisatiemodelconverter draagt zorg voor de vertaling van het centrale autorisatiemodel naar een decentrale. Een voorbeeld is wanneer centraal een procesgericht autorisatiemodel wordt gebruikt en decentrale een functiegericht of afdelingsgericht autorisatiemodel, dan zal hiertussen een vertaalslag uitgevoerd moeten worden. Autorisatiemodel converters/adapters worden toegepast als bijvoorbeeld een autorisatiemodel van een legacysysteem moet worden gekoppeld aan een nieuw centraal autorisatiemodel.
CI4	Autorisatierepository	Een autorisatierepository is de administratie van autorisatiegegevens, bijvoorbeeld de centrale administratie of een doelsysteemadministratie.
CI5	Role Based Access Control-model	Dit model wordt aangeduid met RBAC. Het model is opgebouwd uit rollen, waarbij een rol de autorisaties bevat die nodig zijn voor het uitvoeren van de functie (HR-rol). Een model kan uit een hiërarchie van rollen worden opgebouwd. In dat geval is een rol een set van autorisaties. Gebruikers worden aan de (bovenste laag) rollen gekoppeld en verkrijgen vervolgens de autorisaties die in de betreffende rollen zijn geadministreerd. RBAC gaat uit van het koppelen van identiteiten van gebruikers aan rollen. Voor de identiteitenadministratie wordt meestal de HR-administratie (waaronder het personeelsnummer) als bron gebruikt. Daar een identiteitgegeven per doelsysteem (user-id) kan verschillen, dient in de centrale administratie de relatie te worden gelegd tussen het HR-identiteitsgegeven en de

		doelsysteemidentiteitsgegevens. De ervaring leert dat een rollenmodel uit niet meer dan 2 tot 3 hiërarchische lagen moet worden opgebouwd. Het opzetten en beheren ervan wordt anders te complex. Methoden om een rollenstructuur op te zetten verschillen. Een visie is dat voor een centraal autorisatiemodel geen nieuwe structuur moet worden ontwikkeld, maar dat een autorisatiemodel moet worden gebaseerd op reeds bestaande structuren in de organisatie. Dit model wordt het Business Oriented Autorisatiemodel genoemd (meer informatie zie literatuurlijst). De ervaring bij deze visie is dat dit model goed beheerd kan worden door de betreffende businesspartij. Hierdoor wordt de doelstelling gehaald om autorisatie-management een taak en verantwoordelijkheid van de business te laten zijn. Ook de kosten van de uitvoering liggen op de juiste plaats. Het resultaat is een gebruiksvriendelijk model met lage operationele kosten, zowel voor de business als voor de doelsysteem-beheeromgevingen. Om dit centrale model ook in de doelsystemen door te voeren is vaak een ondoenlijke klus, zeker voor bijvoorbeeld complexe legacysystemen. In dat geval is het nodig een autorisatiemodel converter/adapter toe te passen. Dit kan in sommige gevallen betekenen dat geaccepteerd wordt dat de verschillende autorisatiemodellen rechtstreeks aan elkaar worden gekoppeld, waarbij mismatches geaccepteerd worden. Voor het opbouwen van het model worden bestaande structuren gekozen die reeds in de businessomgeving (doelgroep) bestaan. Voorbeelden van structuren zijn o.a. het organisatiemodel, de bedrijfsprocessen, het functiehuis, een project inrichting, etc.. Van belang is dat de gegevens van de gekozen structuren van goede kwaliteit zijn en bijvoorkeur elektronisch beschikbaar zijn. Het autorisatietoekennings-proces kan dan sterk worden geautomatiseerd. Het rollenmodel kan worden opgebouwd door aan die structuren taken (in de eerste laag) en activiteiten (in de tweede laag) te relateren. Een medewerker kan aan meerdere taken van verschillende structuren worden gekoppeld. Taken bevatten activiteiten. Voor het uitvoeren van activiteiten zijn middelen nodig. Die ‘middelen’ zijn dan o.a. autorisaties, maar kunnen ook fysieke middelen zijn (bijvoorbeeld een laptop of toegang tot een ruimte). De taken bevatten de autorisaties.

		Een andere visie voor het opzetten van een rollenmodel is het koppelen van medewerkers aan een taakrol (op basis van de functie en een persoonlijke rol). Het streven moet dan zijn de inhoud van de persoonlijke rol zo beperkt mogelijk te houden. Ook in deze expertbrief geven we aandacht aan het aspect 'aantal rollen'. Er wordt nogal eens gesteld dat RBAC in de praktijk een te groot aantal rollen oplevert, waardoor de beheersbaarheid haast ondoenlijk wordt. Dat is inderdaad het geval als rollen zelf niet een 'logische eenheid' zijn. Tot nu toe worden RBAC-autorisatiemodellen opgezet vanuit de visie 'wat hebben de gebruikers aan gelijke autorisaties waar we een rol van kunnen maken'. Het resultaat is een complexe set van rollen, waarvan de inhoud een toevallige set van gelijke autorisaties is. De rol bevat een 'rommeltje' aan autorisaties. Dit is o.a. het resultaat van roleminingsmethoden (zie CB16). De praktijk wijst uit dat een dergelijke rollenstructuur onbeheerbaar is en dat het dan een probleem wordt als het aantal rollen groot wordt. Business Oriented Autorisatiemodellen blijven wel beheerbaar. Het aantal rollen doet er niet echt toe. De inspanning voor het wijzigen van een rol is door de logische structuur namelijk minimaal. Gebleken is dat het beleggen van roleigenaren en autorisatie-eigenaren soepel beheer stimuleert. In de rollen moeten functiescheidingsprincipes worden opgenomen. Hiervoor is het nodig dat geadministreerd is welke autorisaties strijdig met elkaar zijn. Er kan voor worden gekozen om strijdigheid in autorisaties over te nemen in de rollen. Deze rollen mogen dan niet aan dezelfde gebruiker worden gekoppeld. Bij een hiërarchisch model moet de rolstrijdigheid dan worden overerft. In dat geval krijgt de gebruiker dus meteen een hele rol(keten) niet als één autorisatie strijdig is. Dat is niet altijd de bedoeling. Daarom zijn er andere oplossingen bedacht om hier mee om te gaan, zie bijvoorbeeld het artikel 'RBAC Next generations' (zie literatuurlijst). Voor en heldere beheerbaarheid is het van belang dat een strakke naamgevingsconventie voor rollen voor bepaald. Deze moet o.a. bevatten hoe de naam van een rol wordt opgebouwd en hoe de vertaling van technische autorisatietaal in de doelsystemen naar businesstaal in

		het centrale autorisatiemodel wordt geregeld. Bij het starten van een access managementproject wordt vreemd genoeg al vaak in de projectopdracht meegegeven dat het autorisatiemodel op basis van RBAC moet worden opgezet. Dat geeft aan dat RBAC inmiddels een goed ingeburgerde term is, maar, zoals al eerder aangegeven, wellicht kan beter een goed beheerbaar autorisatiemodel worden opgebouwd uit meerdere autorisatiemodellen. Dat betekent dat een centraal autorisatiemodel een combinatie kan zijn van bijvoorbeeld RBAC met andere modellen.
CI6	Rule Based Access Control-model	Rule Based Access Control wil zeggen dat op basis van (business) regels autorisaties aan gebruikers worden gekoppeld. Het aanpassen van de regels leidt tot aanpassingen in verstrekte autorisaties. Om dit mogelijk te maken moeten ook hier de gegevens waar de rules op worden gebaseerd goed beschikbaar zijn (hoge kwaliteit en bijvoorkeur elektronisch). Ook hier zijn voor de gegevens de juiste authentieke bronnen nodig. De ervaringen met betrekking tot beheerbaarheid van de rules zijn positief, met dien verstande dat dit vooral goed te gebruiken is voor generieke autorisaties, bijvoorbeeld voor autorisaties die in aanmerking komen voor ‘broad empowerment’ (autorisaties waar ‘iedereen’ over mag beschikken). Rule Based Access Control kan ook worden toegepast op rollen. In plaats van alleen één autorisatie wordt een set van autorisaties dan automatisch toegekend. Dit levert een prima werkbare combinatie van de twee modellen. De ervaring is wel dat het beheren van rules niet eenvoudig door ‘iedereen’ in de business is uit te voeren en dat derhalve het beheer dient te worden belegd bij een business afdeling met specifieke kennis van zaken.
CI7	Policy Based Access Control-model	PBAC is het verstrekken van autorisaties op basis van beleidspolicies. Beleidsregels worden vertaalt naar autorisaties. Het beheer van policy-regels ligt vaak bij security management. Met name in een rule based omgeving kan dit goed worden toegepast.
CI8	Context Based Access Control-model Of Claims Based Access Control-model	CBAC houdt in dat autorisaties niet aan een identiteit zelf zijn gekoppeld, maar aan de eigenschappen van een identiteit. Identiteiten worden voorzien van contextuele gegevens, ook wel entitlements genaamd. Een entitlement is bijvoorbeeld de functie van de identiteit-eigenaar. Bij een gebruikersactiviteit wordt op basis van de entitlements, het toegangsniveau bepaald (en dus niet op

		basis van de identiteit zelf). De uitvoering is derhalve op basis van rules. Bijvoorbeeld: een accountmanager mag klantgegevens lezen.
CI9	Audit Based Access Control-model	ABAC is een methode op basis van controle achteraf. Iedereen mag alles, echter worden wel alle gebruikersactiviteiten gelogd. Indien daar noodzaak voor is kunnen de loggings achteraf worden gecontroleerd. Deze methode is goed van toepassing in omgevingen met een open cultuur. Bijvoorbeeld in een ziekenhuis moeten in een noodgeval alle gegevens van een patiënt opgevraagd kunnen worden. Eventueel kan achteraf worden nagegaan of dit ook echt nodig was.
CI10	Autorisatie classificatieadministratie	Om autorisaties conform beleid te verstrekken kan een autorisatieclassificatiemehode worden gehanteerd. Zo kunnen gevoelige autorisaties concreet worden gemarkeerd en het gebruik ervan worden gemonitord door bijvoorbeeld auditrapportages te filteren op een bepaalde categorie autorisaties. Voorbeelden van classificatie zijn: zeer gevoelig, gevoelig, standaard, ongevoelig. Deze methode wordt vaak op data toegepast (dataclassificaties) en zou derhalve kunnen worden doorgetrokken naar de autorisaties tot die data.
CI11	Identity repository	Een Identity repository is de opslag van identiteiten en/of gegevens per identiteit (bijvoorbeeld persoonskenmerken). Aan de hand van deze gegevens wordt de toegang in doelsystemen vrijgegeven. Vaak is de HR-database de bron voor identiteitgegevens en bijbehorende gegevens van de medewerker. Er is echter niet altijd sprake van één identiteitenbron. Bijvoorbeeld in federatieve omgevingen beschikken verschillende bronnen over identiteit gegevens . Naast de gegevens van een identiteit moeten ook de bijbehorende user-id's worden vastgelegd.
CI12	Rule repository	Bij het toepassen van Rule Based Access Control moet er een rule repository (opslag van de regels) worden aangelegd en beheerd.
CI13	Policy repository	Toegepaste beleidsregels worden opgeslagen in een policyrepository.
CI14	Goedkeuringsadministratie	Wanneer autorisatieaanvragen een goedkeuringsproces doorlopen, moeten deze goedkeuringen worden opgeslagen, zodanig dat deze goedkeuringen voor autorisatiebeheerders en auditors inzichtelijk zijn.
CI15	Loggingadministraties	Gebruikersactiviteiten in de doelsystemen worden opgeslagen in loggingadministraties. Loggingadministraties worden omgezet in loggingrapportages, bijvoorbeeld door autorisatieactiviteiten eruit te filteren, deze te totaliseren

		en opvallende activiteiten expliciet weer te geven. Deze loggingrapportages worden gebruikt om te controleren op frauduleuze pogingen. Deze administratie legt de verbinding met compliance.
CI16	Systeem en applicatie administratie	Systemen, applicaties en andere data area's dienen te zijn geadministreerd. Deze administratie is een basis voor de autorisatiecatalogus. De werking/bedoeling van deze items dient functioneel te zijn beschreven en te zijn voorzien van namen of gegevens van eigenaren (direct of indirect (taaknaam)).
CI17	Autorisatiecatalogus	Om autorisaties te kunnen aanvragen, moet men wel weten welke autorisaties beschikbaar zijn. Deze kunnen via een catalogus in een voor de business begrijpelijke taal beschikbaar worden gesteld. Een catalogus bevat alle autorisaties in alle systemen, met een business naam, technische naam, en een functionele beschrijving. De catalogus kan eventueel ook worden gebruikt om autorisatieclassificatiegegevens op te slaan. De vertaling van techniek naar businesstaal is een beheeractiviteit.
CI18	Gebruikersinterface (rapportages en schermen)	Access management is het beheren van een enorme hoeveelheid aan gegevens die op een juiste wijze en in de juiste samenstelling moet kunnen worden getoond aan de juiste personen. Het kunnen verzamelen van de gegevens en het definiëren van gebruiksvriendelijke schermen en rapportages vraagt de nodige aandacht in het architectuurontwerp. Een vraag hierbij is wanneer gegevens in een scherm en wanneer gegevens in een rapportage moeten worden weergegeven. In vroeg stadium van een project moet hierover goed worden nagedacht. Gekeken moet worden vanuit alle taken in de autorisatiebeheerprocessen. Gebruiksvriendelijkheid, frequentie van gebruik en kwaliteit van de gegevens bepalen onder andere de uitvoering van de interface. Sommige gegevenscombinaties zijn lastig samen te stellen en moeten in nachtverwerkingen worden opgebouwd. Denk hierbij aan een Soll-Ist rapportage van de autorisaties per medewerker.

24 Technische componenten

Technische componenten zorgen dat de bovengenoemde componenten kunnen worden gerealiseerd. De belangrijkste technische componenten zijn: gegevensopslag, de gegevens-overdracht en de gegevensweergave (schermen en rapporten).

De volgende technische componenten zijn onderkend:

Nr	Component, product, onderwerp	Omschrijving
CT1	Gegevens databases	De genoemde repositories zijn in de betreffende systemen meestal een locale database. Autorisaties die in code zijn opgenomen, maken de applicatie moeilijk onderhoudbaar. Deze databases dienen te zijn voorzien van een goede beveiliging en encryptie.
CT2	Provisioningssysteem	Provisioning is de uitwisseling van autorisatiegegevens tussen een centrale autorisatieadministratie en een doelsysteem. Krijgt een gebruiker een autorisatie toegewezen, of moet deze worden ingetrokken, dan wordt vanuit het centrale systeem met de centrale administratie een opdracht gestuurd (geprovisioned) naar het doelsysteem. Ook kunnen rapportage opdrachten worden verstuurd, bijvoorbeeld om Ist-gegevens van een doelsysteem op te vragen. Dit wordt ook wel reconciliation genoemd.
CT3	Provioningsprotocol	Gegevensoverdracht tussen componenten vindt plaats via protocollen. Voor autorisatiegegevens is dat het provisioningsprotocol. Een vraag is of daarvoor (open) standaards moeten worden gebruikt. Het antwoord is in principe 'Ja', in verband met de compatibiliteit met andere systemen. Echter zijn standaarden soms omgevings-afhankelijk. Denk bijvoorbeeld aan een cloud-omgeving. Legacysystemen zouden moeten worden voorzien van een converter/adapter die een (open) standaard protocol aan kan. De belangrijkste standaarden zijn op dit moment LDAP (tussen systemen onderling) en SAML of SPML in Federatieve omgevingen. Dit zijn protocollen gericht op autorisatie en/of op authenticatie. Nieuwere protocollen praten op een 'hoger niveau'. Deze worden 'policybased' protocollen genoemd. Een voorbeeld hiervan is XACML.
CT4	Sessie beheer component	In een webomgeving kunnen ook autorisatiegegevens die horen bij een sessie tijdelijk in de PC worden opgeslagen.

		Bijvoorbeeld als het gaat een Single Sign On functionaliteit tussen meerdere webdiensten. De gegevens worden dan vaak opgeslagen in cookies e.d..
CT5	Workflow component	De beschreven processen worden ondersteund door tooling. In de tooling moeten derhalve workflow-componenten aanwezig zijn die voorzien in de betreffende lifecycles van de gegevens.

BENEFITS ARCHITECTUURCOMPONENTEN

Een architectuurcomponent kan op verschillende manieren worden uitgewerkt. De wijze waarop het wordt uitgewerkt bepaald hoeveel tijd en geld het kost om deze te realiseren. Om de inspanning en kosten per component in balans te laten zijn met de doelstellingen van het bedrijfsbeleid, is het handig inzicht te hebben in de benefits per component. Dit inzicht verscherpt het denken en het maken van afwegingen over welke componenten belangrijk zijn en in welke mate deze moeten worden uitgewerkt.

In de eerst expertbrief zijn de benefits van access management beschreven. In deze sessie worden deze gekoppeld aan de in de voorgaande tabellen beschreven componenten.

Bij het doorvoeren van verbeteringen in een access management omgeving, is een eerste stap het vaststellen welke benefits belangrijk zijn voor het realiseren van het (security)-ambitieniveau van de organisatie (of verbeterprogramma). Deze vaststelling leidt vervolgens tot keuzes als: wel of niet opnemen in een verbeterproject, welke diepgang van uitwerken wordt nagestreefd, welke prioriteit wordt toegekend, wordt het in een keer of gefaseerd geïmplementeerd (middels bijvoorbeeld plateaudefinities in het project), etc.. Deze keuzes worden mede bepaald door haalbaarheid binnen het programma: wat is haalbaar in een reële periode en binnen reëel budget. Wat levert het op met betrekking tot het ambitieniveau.

Alle componenten zijn in meer of mindere mate nodig voor een goed werkend autorisatiemanagement, maar de mate van uitwerking kan ook stapsgewijs groeien van de huidige, of tijdelijke eenvoudige, situatie naar een professionele. Het gaat erom dat bewust de component invullingskeuzes worden gemaakt.

Onderstaande matrix kan als handvat worden gebruikt om inzicht te krijgen welke benefits voor welke componenten van toepassing zijn. Deze tabel moet worden gezien als slechts een globale richtlijn of als praatplaat om de discussies over benefits te ondersteunen. Het is zeker niet volledig of voor iedere situatie te gebruiken. Het is slechts een handreiking en die moet naar eigen inzichten worden toegepast.

26

Algemene baten versus architectuurcomponenten

Nr en omschrijving benefits uit expertbrief 1		Mapping op nr's
BA1	Beter IT portfoliomanagement (inzicht in gebruikte systemen en applicaties).	CI16, CI17
BA2	Er is concreet en snel inzicht in benodigd aantal licenties.	CB7, CI10, CI18
BA3	Kostendoorbelasting kan eenvoudig plaatsvinden en concreet worden gemaakt.	CB7
BA4	Doordat autorisaties meer consistent zijn zal het aanvraagpatroon stabieler zijn.	CI1, CI5..CI9
BA5	Het aanvragen kost de business en de beheerorganisatie minder (doorloop)tijd.	CC1..CC3, CB2..5, CB8, CB9, CB12..15
BA6	Auditprocessen nemen minder tijd in beslag door betere rapportages.	CC6, CC7, CB6, CI1, CI10, CI14, CI15, CI18
BA7	KPI doelstellingen kunnen eenvoudiger worden gedefinieerd en geverifieerd.	CC5..CC7
BA8	Het is goed voor het bedrijfsimago als gecommuniceerd kan worden dat de goed ingerichte autorisatiebeheerorganisatie invulling geeft aan de van toepassing zijnde wet & regelgeving. Omgekeerd heeft een calamiteit een zeer nadelige invloed op het bedrijfsimago en de commerciële activiteiten. De kans dat dit gebeurt, bijvoorbeeld in de vorm van fraude, wordt beperkt met goed ingericht autorisatiebeheer .	CC1..CC7, CB6, CI1, CI15, CI18
BA9	Gestructureerde en/of vereenvoudigde autorisatie activiteiten kunnen in aanmerking komen voor outsourcing wat kostenbesparing kan opleveren.	CC1..CC7, CB1..CB13, CI11..CI18, CT1..CT3
BA10	Doordat alle verschillende aanvraagprocessen en ondersteunende middelen (tooling) worden gecentraliseerd en centraal gefaciliteerd (één tool), worden de beheerkosten lager: • door minder mensen kan hetzelfde werk worden gedaan; • processen kunnen deels worden geautomatiseerd; • maar één tool i.p.v. meerdere (minder beheer); • één uniforme werkwijze voor de gehele organisatie (efficiënte communicatie en minder servicedesk ondersteuning); • minder handmatige handelingen (doorzetten van aanvragen, het aanbrengen van autorisaties de terugkoppeling communiceren naar de aanvrager).	CB1..CB13, CT1..5
BA11	De business kan sneller de juiste autorisaties aan medewerkers toe laten kennen. Daardoor kan een nieuwe medewerker sneller met al zijn autorisaties aan de slag en kunnen wijzigingen in autorisaties sneller worden doorgevoerd, zonder teniet te doen aan juiste administraties en goedkeuringen. De agility (flexibiliteit) is hoog.	CB3, CB4, CB12..15, CI1, CI5..CI9

BA12	Bij goed ingericht access management is het aanbrengen van SSO eenvoudig, waardoor de gebruikers minder vaak hoeven aan te loggen.	CI1, CI5..CI11, CT2, CT3
BA13	Doordat het autorisatiemanagement uniform en eventueel centraal geregeld is, is het eenvoudiger om doelgericht of gefaseerd nieuwe applicaties of systemen uit te rollen in de business.	CB9..CB11, CI1..CI14, CI16, CI17, CT1..CT3
BA14	Een access management implementatie zal het centraliseren en uniformeren van bronnen (als personeels-, doelsysteem-, applicatie-, project-, of proces-administraties) stimuleren.	CI1..CI17
BA15	Vaak zijn de autorisatiemodellen op doelsystemen zeer verschillend of onvoldoende gedefinieerd (langzaam ontstaan). Een access management project zal stimuleren eenzelfde autorisatiemodel na te streven op alle doelsystemen.	CI1..CI17
BA16	Goed ingericht autorisatiemanagement draagt bij aan continuïteitsvraagstukken, bijvoorbeeld doordat bij een uitwijksituatie gebruik kan worden gemaakt van de centrale autorisatieadministratie i.p.v. alle lokale doelsysteemadministraties.	CI1..CI17, CT1

Baten m.b.t. compliance versus architectuur componenten

Nr en omschrijving benefits uit expertbrief 1		**Mapping op nr's**
BC1	Inzicht in autorisatie-afkeuringen.	CB3, CB4, CB9, CB14, CI14, CI18
BC2	Minder foutieve autorisatie-toekenningen.	CB1..CB13, CI1
BC3	Men snapt beter welke autorisaties men aanvraagt en waarom.	CI1..CI17
BC4	Auditprocessen kunnen direct worden gericht op gevoelige autorisaties.	CB6, CI1, CI4..13, CI15..17
BC5	Controle op fraude wordt makkelijker.	CB6, CI1, CI4..13, CI15..17
BC6	Door geautomatiseerde controles (bijv. Ist-Soll vergelijking) worden 'achterdeur'-processen in de kiem gesmoord.	CB6, CB16, CI11, CI15, CI18, CT1..CT3
BC7	Niet alleen de kans op fraude wordt verkleind, ook de controle op intellectuele eigendommen wordt beter en effectiever controleerbaar. Hierdoor is de kans kleiner dat informatie bij de concurrent of in de media terecht komt.	CB6, CI1, CI4..13, CI15..17
BC8	Omdat beter (continue) inzicht is in de juistheid van de verstrekte autorisaties, is de verleiding kleiner om bewust foutieve autorisaties aan te vragen.	CB3, CB6, CB9, CI1..CI14, CI18
BC9	Functiescheidingsregels kunnen direct bij de start van het aanvraagproces worden gemanaged (bijvoorbeeld door functiescheidingsregels op te nemen in het autorisatiemodel). In een applicatie zelf gebeurt dit pas op	CC7, CB3, CB6, CI1..CI14

	het moment dat een identiteit wordt geautoriseerd, of het gebeurt achteraf bij audits (bijvoorbeeld met behulp van businessrules-tools).	
BC10	Vaak worden door de implementatie van access management meerdere organisatorische vraagstukken concreet. Een belangrijk vraagstuk gaat over het beleggen van het 'eigenaarschap'. Voor systemen en rollen moeten eigenaren worden benoemd. Bij een bedrijfsprocesgerichte aanpak moeten proceseigenaren worden aangewezen. Zo worden verantwoordelijken expliciet en inzichtelijk.	CC1..CC3, CB13, CI14
BC11	Door het snel verstrekken van autorisaties neemt de behoefte aan non-personal accounts af.	CB3..CB6

LESSONS LEARNED ARCHITECTUUR

In de werkgroepsessie zijn de volgende lessons learned besproken:

Nr	Omschrijving
LL1	Niet beginnen met het aanschaffen van een IAM-systeem voordat goed is nagedacht over wat je wilt. Op een of andere manier komt het regelmatig voor dat de keuze voor een systeem al is gemaakt of het systeem al is aangeschaft, voordat het IAM-programma is gestart. De functionaliteiten die IAM-systemen bieden en de architectuur zijn behoorlijk verschillend. Eerst moet bijvoorbeeld zijn vastgesteld uit hoeveel lagen het autorisatiemodel zal worden opgebouwd en welke IAM-systemen/leveranciers dat ondersteunen. Ook moet worden vastgesteld of de doelsystemen met automatic provisioning direct op het IAM-systeem gaan worden aangesloten.
LL2	Zorg ervoor dat consensus is bereikt over de governance vraagstukken. Deze kunnen zeer bepalend zijn voor de te kiezen aanpak en oplossing. Zorg dat eerst duidelijk is hoe de taken en verantwoordelijkheden gaan worden belegd (RACI). Bijvoorbeeld wat zijn de taken van een HR-afdeling? Zijn zij of bijvoorbeeld de afdelingsmanagers verantwoordelijk voor de inhoud van de brongegevens (personeelnummer, plaats in de organisatie, etc.) in het HR-systeem?
LL3	Start een IAM-programma vanuit de business en niet vanuit de techniek of IT.
LL4	Access management is complex en architectuur kan heel abstract zijn. Dat zijn twee ingrediënten die ervoor kunnen zorgen dat er een groot gat ontstaat tussen de feitelijke doelstellingen en de uiteindelijke oplossingen. De ruimte voor interpretatieverschillen is groot. Maak daarom architectuur concreet. Zorg dat de stip aan de horizon (als ambitieniveau) duidelijk geformuleerd is. De stap van architectuur naar functioneel en technisch ontwerp moet klein zijn anders worden keuzes en oplossingen alsnog vanuit verschillende visies gemaakt. Dit is een wat algemeen statement, maar het is zeker ook bij access management van toepassing.
LL5	Zet een access management programma gefaseerd op. Definieer haalbare plateaus waarbij de uiteindelijke doelstellingen via meerdere iteratieslagen worden gehaald. Maak in iedere iteratie slechts kleine stappen. Werk hierbij zowel top-down als bottom-up. Het is een kunst de doelstellingen per plateau zo beperkt mogelijk te houden!
LL6	Van zowel de architectuur als de feitelijke uitwerking moet het volwassenheidsniveau kunnen groeien. Denk hierbij aan voortschrijdend inzicht wat bij access management programma vaak in ruime mate aanwezig is.
LL7	Een autorisatiemodel is doelsysteem gerelateerd. Zorg ervoor dat de doelsysteem autorisatiemodellen kunnen worden aangesloten op een centraal autorisatiemodel of dat deze op gecontroleerde wijze naast elkaar kunnen worden gebruikt. Zo heeft bijvoorbeeld een mainframe een strakke autorisatiestuctuur waarin een RBAC-oplossing prima past (statisch model), terwijl een SOA-omgeving gebaseerd kan zijn op een claim based structuur (dynamisch model).
LL8	Beperk het aantal typen rollen en probeer deze zoveel mogelijk geautomatiseerd toe te kennen, bijvoorbeeld op basis van de functie van de medewerker. Neem daarbij wel de ‘operationele’ functie en niet die uit het HR-functiehuis. Het HR-functiehuis beschrijft meestal een functie op een te hoog abstractieniveau (dezelfde functie kent meerdere uitvoeringsvormen). Voor automatische toekenning moet wel de

	operationele functie in het HR-bron systeem zijn opgenomen. Een mogelijke uitvoeringsvorm van een autorisatiemodel is door aan iedere medewerker één functierol en één persoonlijke rol toe te kennen. Probeer daarbij de persoonlijke rol zo leeg mogelijk te houden.
LL9	Rollen hoeven niet statisch te zijn. Door het regelmatige evalueren van de rollen kunnen optimalisaties worden doorgevoerd.
LL10	Zorg in de eerste plaats dat taken, bevoegdheden en verantwoordelijkheden goed zijn belegd (RACI), dat geldt met name voor het aanwijzen van gegevenseigenaren (permissie-eigenaar). Op het moment dat eigenaarschap goed is ingeregeld kunnen discussies over toegang tot gegevens efficiënt worden gevoerd.
LL11	Belast de business niet te veel, te zwaar of onnodig met het access management programma of überhaupt met autorisatievraagstukken. Doe het één keer intensief of juist heel gedoseerd, zodat men er niet ‘moe’ van wordt.
LL12	Probeer in een access management programma niet in één keer alle quickwins te oogsten, maar streef per fase een beperkt aantal doelen na. Stel hiervoor een groei scenario op.
LL13	Probeer niet in één keer alle onderdelen van de access management organisatie opnieuw in te richten, maar breng stap voor stap verbeteringen aan in de bestaande situatie, in de richting van het beoogde ambitieniveau en architectuurmodel. Richt je daarbij in beginsel op de haalbare kwaliteit van het component, als bijvoorbeeld de actualiteit, volledigheid en beschikbaarheid van het administratieve onderdeel.
LL14	Probeer in een access management programma voor elk component zichtbare resultaten te boeken, door bijvoorbeeld een quick win te realiseren. Daarmee houd je de betrokkenen geïnteresseerd en blijft er aandacht voor het programma. Dit geldt generiek voor programma’s, maar maak voor access management programma’s gebruik van de genoemde benefits in de eerste expertbrief over Access Management.
LL15	Beschrijf de componenten vanuit de visie van iedere RACI-rol (verantwoordelijkheden). Betrek de betreffende medewerkers in de visievorming die daar aan vooraf gaat. Dit maakt de beschrijving volledig(er) en stimuleert de motivatie van de betrokkenen.

CONCLUSIES EN VERVOLG

De leden van deze expertgroep, zie bijlage 2, hebben antwoorden geformuleerd op de gestelde vragen. Het beoogde resultaat is daarmee gehaald. De ontwikkelingen op dit vakgebied staan echter niet stil, zowel technologisch als qua visie. Deze expertbrief zal derhalve onderhavig zijn aan voortschrijdend inzicht.

De leden van de expertgroep zijn daarom altijd geïnteresseerd in opmerkingen of nieuwe inzichten en nodigen u van harte uit om deze kenbaar te maken. U kunt uw reacties sturen naar expertbrief@pvib.nl. Ook indien u deze expertbrief heeft kunnen waarderen stellen de deelnemers een e-mailtje zeer op prijs!

Hoe verder?
Zoals eerder aangegeven is het onderwerp access management opgesplitst in 4 sessies met ieder een eigen set aan onderwerpen, zie bijlage 1. Ook de resultaten hiervan worden middels expertbrieven verwoord en via de site van het PvIB beschikbaar gesteld.

Ook via de site www.ibpedia.nl kunt u meewerken aan verdere verrijking en kennisdeling over access management en andere onderwerpen met betrekking tot informatiebeveiliging. Iedereen is van harte uitgenodigd om hieraan deel te nemen.

32 LITERATUURLIJST

De expertgroep beveelt ter aanvulling of ter verdieping van de behandelde onderwerpen de volgende literatuur aan:

Main bodies:

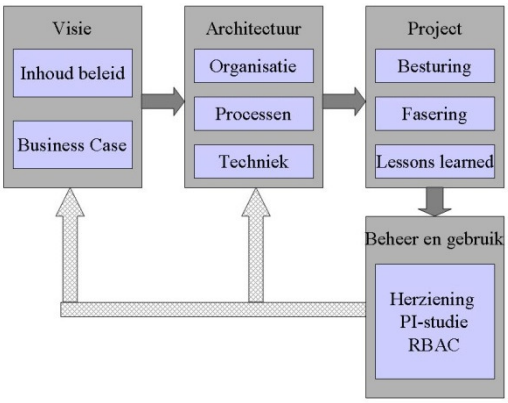
- Expertbrief “Access management deel1:Visie”, zie https://www.pvib.nl/expertbrief
- Expertbrief “security architectuur”, Jaargang 2, nr4, december 2006, zie https://www.pvib.nl/?page=6259972
- Studie Role Based Access Control http://www.pvib.nl
- NIST reeks http://csrc.nist.gov/
- OSA, open security architecture
- Enterprise Access Management http://www.jpvincent.nl/BIAMEIA

Artikelen:

- Business Oriënted Autorisatie Model , maart 2010
- RBAC Next generations https://www.pvib.nl/download/?id=6474402&download=1
- ABAC https://www.pvib.nl/download/?id=6474160&download=1
- ABAC https://www.pvib.nl/download/?id=6474183&download=1
- CBAC https://www.pvib.nl/download/?id=10511450&download=1

BIJLAGE 1. SESSIE-OVERZICHT EXPERTBRIEVEN ACCESS MANAGEMENT

Aanpak
De voorbereidingsgroep wil producten opleveren van een hoog kwaliteitsgehalte binnen een reëel tijdsbestek en heeft daarom het onderwerp access management in vier hoofdgebieden opgesplitst (zie figuur 1). Deze hoofdgebieden worden in gescheiden sessies besproken en vallen samen met de stappen die doorlopen moeten worden wanneer men met access management aan de slag wil gaan. Per hoofdonderwerp wordt een expertbrief opgeleverd. Iedere expertbrief kan in principe resulteren in aanvullende themasessies, vervolgartikelen en handreikingen, afhankelijk van de belangstelling en het animo onder deskundigen om hierin te participeren.



Figuur 5. Opsplitsing van onderwerp access management in 4 expertbrieven.

De vier hoofdgebieden behelzen het volgende:

1) Visie: Het eerste onderdeel betreft het vormen van een visie over het daadwerkelijk bestaan van één ideaal access management concept. Start een ideaal concept met het hebben van concreet beleid en wat die moet die beschrijven? Het realiseren/implementeren van een compleet access management-concept zal, als gevolg van kosten (businesscase) of complexiteit, niet altijd volledig of in één keer haalbaar zijn. Welke risico's worden onderkent die het succes van een implementatieproject kunnen tegenwerken.

2) Architectuur (deze expertbrief): In het tweede onderdeel wordt access management vanuit architectuur beschreven. Zowel contextueel, als de aspecten omtrent organisatie- en procesinrichting, autorisatiemodellering en techniek.

3) Projectmanagement: In het derde onderdeel zal worden beschreven hoe de implementatie kan worden gerealiseerd en welke werkwijzen en projectinrichtingen daarbij kunnen worden toegepast.

4) Beheer en gebruik: Het vierde onderdeel richt zich op de operationele situatie. Het beantwoord de vraag hoe een beheerorganisatie er concreet uit kan zien, welke ervaringen zijn opgedaan met beschikbare hulpmiddelen, etc. Ook kan, als gevolg de activiteiten van de expertgroepen, de visie op access management zodanig zijn ontwikkeld dat de PI-studie RBAC nader kan worden aangepast.

BIJLAGE 2. INFORMATIE OVER DE DEELNEMERS

Onderstaande deelnemers hebben bijgedragen aan deze expertbrief. Mocht u met een van hen contact willen opnemen dan kan dat via het secretariaat van het PvIB, zie http://www.pvib.nl/contact.

Jean-Pierre Vincent

Vervult rollen als projectmanager, architect en analist in identity & access management-programma's bij grote instellingen in de financiële en telecom branche. Bij zijn werkgever is hij thougtleader identity & access management.

Karin van de Kerkhof

Heeft als consultant ervaring met identity&access management projecten in de overheids- en financiële sector. Is verder werkzaam als auditor.

Ben Elsinga

Is als consultant werkzaam op het vakgebied van identity en access management en enterprice architectuur in met name de overheidssector

Jan-Roel Löwenthal

Is voornamelijk werkzaam in de overheidssector. Houdt zich bezig met Servicemanagement, Architectuur en Informatiebeveiliging. Is bij zijn werkgever focus arealeader van de community identity & access management en heeft op dat vakgebied bij verschillende klanten ervaring opgedaan.

Andre Koot

Is als security manager bekent met het vakgebied identity en access management. Daarnaast is hij auteur van diverse artikelen over access management ontwikkelingen.

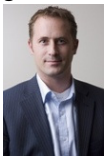
Damiën Meijer

Is als consultant werkzaam op het vakgebied van identity en access management.

Henk Bel

Is als security consultant betrokken bij verschillende identity en access management projecten. Heeft een focus op business aspecten, governance en architectuur en is bij zijn werkgever verantwoordelijk voor de vakontwikkeling van het identity en access management domein.

John van Westeneng



Is als IAM consultant, architect en projectmanager werkzaam in verscheidene identity en access management projecten in Nederland en België.

Karel van Oort

Is als security consultant betrokken geweest bij verscheidene identity en access management projecten.

Piet Kalverda

Is als security consultant werkzaam in de financiële sector en is betrokken bij de implementatie van identity en access management.

Wiyaykumar Jharap

Is als consultant en projectmanager betrokken bij IAM-implementaties in de industriële en semi-overheidssector.

Als reviewer heeft bijgedragen:

Renato Kuiper

Is management consultant en richt zich op het snijvlak van informatiebeveiliging, risicomanagement en architectuur. Vanuit die invalshoeken heeft hij veel ervaring opgedaan in Identity en Access Management projecten.

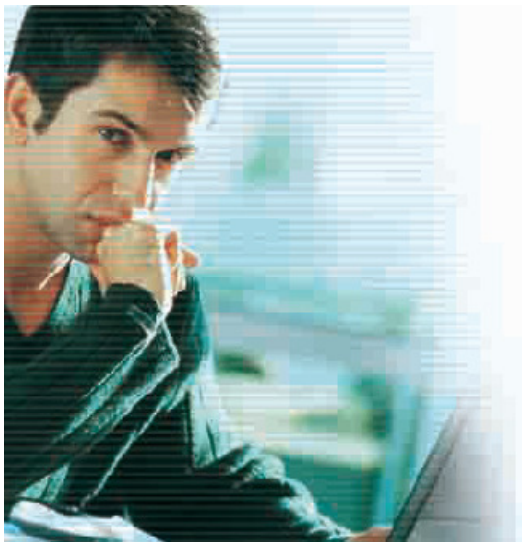
36

APPENDIX GEBRUIKTE LICENTIEVORM

De expertbrief wordt gepubliceerd onder de volgende licentie:
http://creativecommons.org/licenses/by/3.0/nl/

Deze pagina ziet er op het moment van schrijven als volgt uit:

WORDT LID VAN HET PVIB, SPEEL OP ZEKER EN BEVEILIG SAMEN...



Informatiebeveiliging is reeds jaren lang een noodzakelijk, spannend en dynamisch vakgebied. Vrijwel alle beroepen hebben meer dan ooit te maken met vertrouwelijkheid, beschikbaarheid en integriteit van informatie. Of u nu als directeur, manager, adviseur of programmeur werkzaam bent. Het Platform voor Informatiebeveiliging kan u behulpzaam zijn bij al uw vraagstukken op het gebied van informatiebeveiliging.

Wat is het Platform voor Informatiebeveiliging?
Het PvIB is een open, breed samengesteld platform waarin professionals elkaar vinden om professioneel inhoud te geven aan informatiebeveiliging, door het uitwisselen van ideeën, informatie, kennis, inzichten en vooral veel praktijkervaring.

Wat willen wij bereiken?
Wij willen de fysieke, (systeem)technische & organisatorische beveiliging van gegevens en van de gegevensverwerkende middelen tegen inbreuken van binnenuit of buitenaf bevorderen. Ook willen wij de uitwisseling van kennis en ervaring en het netwerken van de in het vakgebied werkzame personen bevorderen. Bijvoorbeeld door middel van deze expertbrief.

De doelgroep
De doelgroep van het PvIB omvat iedereen, die door studie of beroepshalve te maken heeft met informatiebeveiliging, of hiervoor een bijzondere belangstelling heeft. Het snel groeiende ledenbestand kent vele disciplines zoals studenten, informatiearchitecten, technici, managers, organisatieadviseurs, juristen, beveiligingsfunctionarissen en IT auditors. Onze leden komen voort uit alle mogelijke opleidingen, bedrijven, overheden, organisaties en leveranciers.

Voor de diverse soorten van lidmaatschap verwijzen wij u gaarne naar:

https://www.pvib.nl/abonnementsinformatie