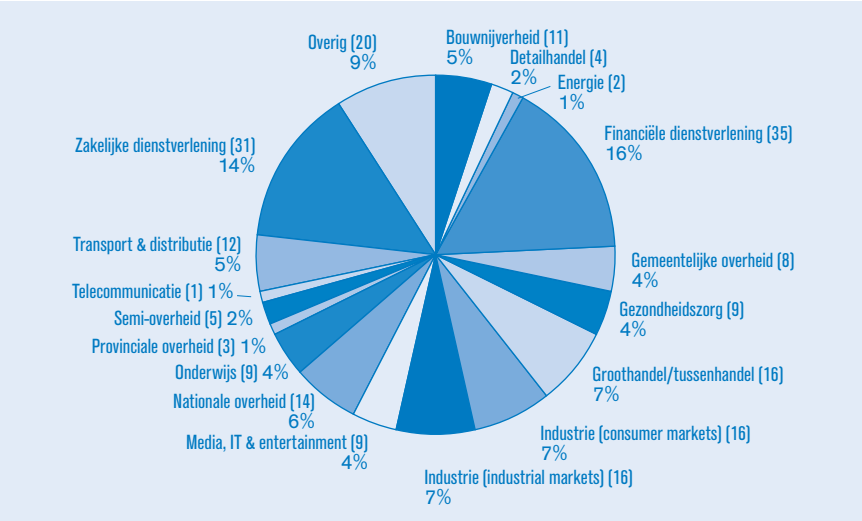
Identity Management: hoe (on)toereikend is het nu en hoe kan het beter?

Drs. ing. R.F. Koorn RE en ing. J.A.M. Hermans RE

De situatie in Nederland op Identity Management-gebied laat vele knelpunten zien; organisaties blijken niet 'in control' te zijn. Gedeelde wachtwoorden, silo-oplossingen per applicatie of platform met hierdoor talloze authenticatiemiddelen en wachtwoordregimes, gestapelde autorisaties, doorbroken functiescheiding, weinig inzicht bij het management, hoge helpdeskkosten voor wijzigen van wachtwoorden en autorisaties, etc. De lijst van zwakke punten liegt er niet om. Dit artikel vat de belangrijkste uitkomsten samen van het grootschalige Identity Management-onderzoek dat KPMG heeft uitgevoerd. Inmiddels zijn veel organisaties gestart met het verbeteren van het authenticatie- en autorisatiemanagement, de ingrediënten van Identity Management. Daartoe heeft KPMG Information Risk Management een programma- en projectaanpak ontwikkeld die eveneens in dit artikel beknopt wordt behandeld.

Inleiding

In 2003 heeft KPMG Information Risk Management in samenwerking met het Genootschap van Informatie Beveiligers (GvIB) een onderzoeksvragenlijst inzake Identity Management verstuurd naar bijna 1000 Nederlandse organisaties, in alle publieke en private sectoren. 224 organisaties hebben gereageerd, zodat gesproken kan worden van een representatief beeld van de huidige situatie (zie figuur 1).



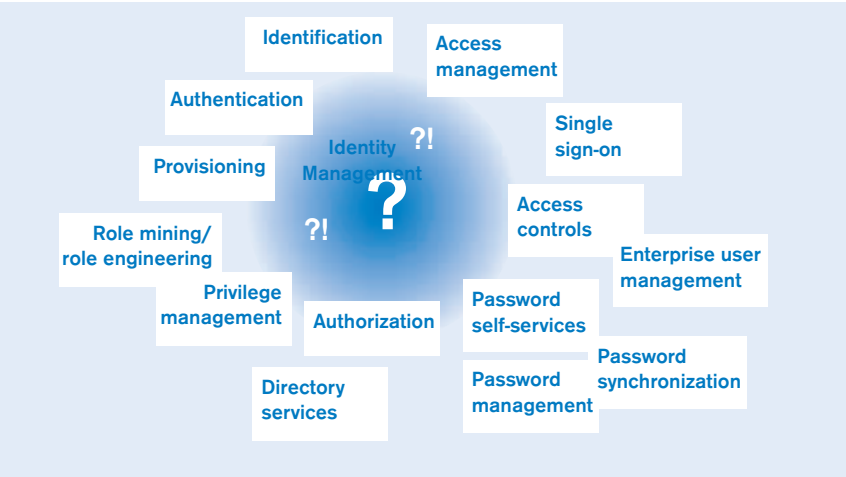
Figuur 1. Respondenten ingedeeld naar sectoren.

Drs. ing. R.F. Koorn RE is partner van KPMG Information Risk Management te Utrecht. Hij richt zich op onderwerpen als informatiebeveiliging, Identity Management, elektronisch factureren, elektronische handtekeningen en betrouwbare internettoepassingen. Hij heeft het hier besproken Identity Management-onderzoek geleid. Verder ontwikkelt hij voor de Nederlandse overheid en de Europese Commissie momenteel het Witboek inzake het toepassen van Privacy Enhancing Technologies.

koorn.ronald@kpmg.nl

Ing. J.A.M. Hermans RE is werkzaam als senior manager bij KPMG Information Risk Management in Amstelveen. Hij is de KPMG National Service Manager voor Identity Management en heeft de laatste acht jaar vele projecten op het gebied van PKI, e-business en Identity Management uitgevoerd bij diverse grote organisaties in en buiten Nederland. Daarnaast leidt hij de internationale productontwikkeling van KPMG ten aanzien van Identity Management, hetgeen heeft geleid tot de overkoepelende KPMG Identity Management in Control-aanpak.

hermans.john@kpmg.nl



Figuur 2. Alfabetsoep rond Identity Management.

Achtergrond Identity Management

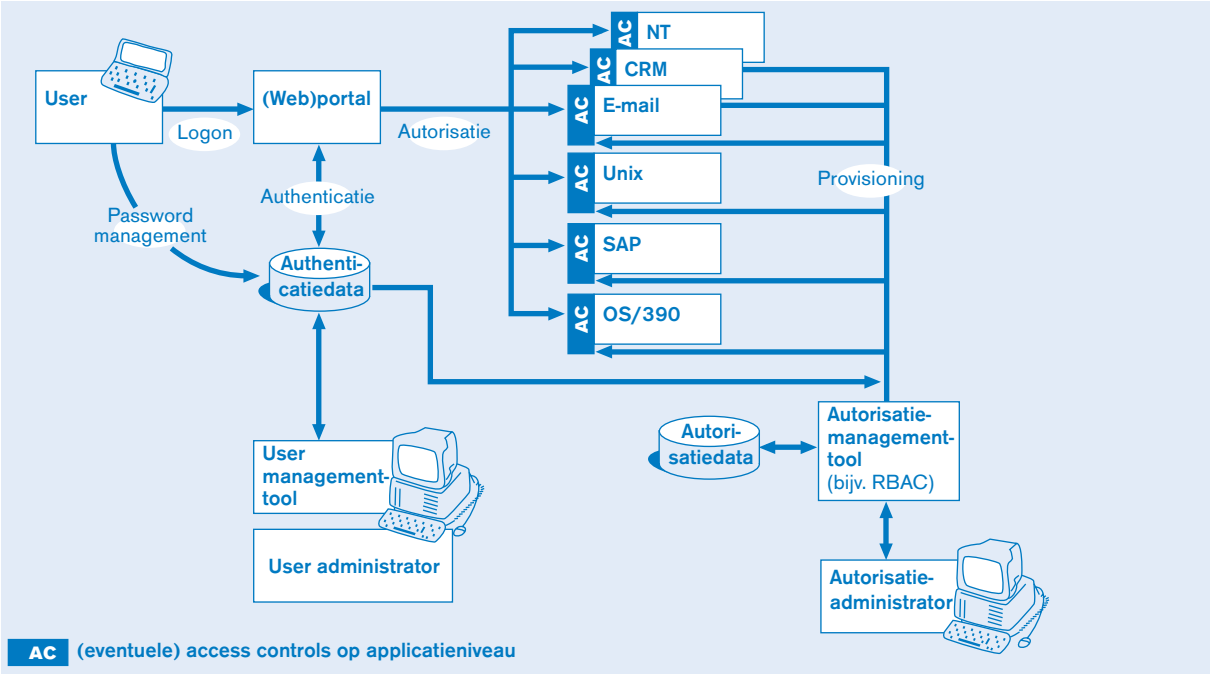
Identity Management is een veelgebruikte term waarmee niet altijd exact hetzelfde wordt bedoeld (zie figuur 2). In feite gaat het om logische toegangsbeveiliging in een eigentijdse vorm. Om onduidelijkheid te voorkomen gaan we in dit artikel uit van de volgende omschrijving:

Identity Management:
Het beleid, de processen en ondersteunende systemen die managen welke personen toegang verkrijgen tot informatie en ICT-middelen en wat ieder persoon gerechtigd is hiermee te doen.

Identity Management omvat het vaststellen en verifiëren van de identiteit van personen c.q. ICT-gebruikers (authenticatiemanagement) en het vaststellen, toewijzen, verifiëren en zo nodig intrekken van toegangsrechten van geauthenticeerde gebruikers tot specifieke systemen en informatie (autorisatiemanagement). Hierbij ondersteunende activiteiten betreffen het beheer van gebruikersgegevens ('user management') en het gebruikers voorzien van authenticatiemiddelen en autorisaties ('provisioning').

Een gebruiker die toegang wil verkrijgen tot een specifiek systeem of bepaalde informatie zal zich eerst eenduidig moeten authenticeren. Dit houdt in dat wordt vastgesteld of deze gebruiker inderdaad degene is die hij zegt te zijn. Na een succesvolle authenticatie zal van deze gebruiker moeten worden vastgesteld tot welke systemen en informatie hij is geautoriseerd toegang te krijgen. Op basis van een samengestelde set van toegekende autorisaties wordt de gebruiker vervolgens al dan niet toegang verleend.

In een praktijkvoorbeeld werkt dit als volgt: een gebruiker wil inloggen op een webportal. Allereerst zal hij zijn identiteit tonen door bijvoorbeeld een gebruikersnaam in te voeren. Om aan te tonen dat zijn gebruikersnaam bij hem hoort zal de gebruiker zich authenticeren met een authenticatiemiddel, bijvoorbeeld door een wachtwoord in te voeren of een smartcard te laten uitlezen. De ingevoerde gebruikersnaam en het bijbehorende wachtwoord worden vervolgens vergeleken met in de authenticatiedatabase (al dan niet versleuteld) opgeslagen gebruikersnamen en wachtwoorden. Deze authenticatiedatabase dient actuele gebruikersgegevens te bevatten. Deze database(s) wordt (worden) veelal onderhouden door ICT-medewerkers, maar in verschillende organisaties (ook) door applicatiebeheerders in de gebruikersorganisatie.



Figuur 3. Voorbeeld van het verkrijgen van toegang tot een webportal.

Zodra de authenticatie succesvol is verlopen krijgt de gebruiker, op basis van actuele gegevens die zijn opgeslagen in de autorisatiedatabase(s), wel of geen toegang tot specifieke via de portal toegankelijke applicaties of informatie (ook een geauthenticeerde gebruiker heeft immers toegang tot bepaalde systemen en gegevens). Dit kan bijvoorbeeld geschieden op basis van deelname van de gebruiker aan een groep, zijn functie of zijn organisatorische rol. Dit laatste wordt Role-Based Access Control (RBAC) genoemd (zie verder het artikel van Heiden c.s. in deze Compact en [Mien03]).

Waarom aandacht besteden aan Identity Management?

Logische toegangsbeveiliging is van belang sinds er informatiesystemen worden gebruikt. Vanwaar dan momenteel de aandacht voor het onderwerp? Redenen hiervoor zijn onder andere:

- de noodzaak van een betere grip en controle op de toegang tot bedrijfsinformatie en systemen vanwege:
  - een explosieve groei van het aantal voor gebruikers beschikbare objecten (applicaties, informatie en systemen) in een geconsolideerde ICT-infrastructuur over een variëteit van kanalen (LAN, WAN, internet, mobiel, wireless);
  - het ontsluiten van de interne ICT-infrastructuur voor externe gebruikersgroepen, zoals klanten, freelancers, leveranciers en businesspartners;
  - de veranderende wet- en regelgeving, waaronder de Wet bescherming persoonsgegevens (Wbp), Sarbanes-Oxley, Tabaksblat en Basel II;
  - de aandacht bij toezichthoudende instanties op het vlak van corporate governance ('goed huisvaderschap');
- de noodzakelijk geachte kostenverlaging door het verminderen van de belasting van helpdeskmedewerkers, applicatie-, systeem- en databasebeheerders alsmede van ICT-auditors;
- het verhogen van de kwaliteit van de ICT-dienstverlening aan de in- en externe klanten, ten aanzien van:
  - gebruikersgemak;
  - toegangsmogelijkheden (24 × 7).

Dit alles met behoud van adequate controle.

Om te kunnen vaststellen hoeveel waarde wordt toegekend aan de inzet van Identity Management is organisaties ook gevraagd in hoeverre Identity Management wordt gezien als 'enabling technology' bij elektronische dienstverlening. Een enabling technology is gedefinieerd als een technologie die bepaalde typen interne of externe dienstverlening en transacties vergemakkelijkt en/of mogelijk maakt (aangaan van een contractuele overeenkomst, aankooptransacties, toegang tot uiterst privacygevoelige gegevens, e.d.). Het grootste deel (76%) van de organisaties ziet Identity Management als enabling technology voor elektronische dienstverlening (zie figuur 4).

Tevredenheid

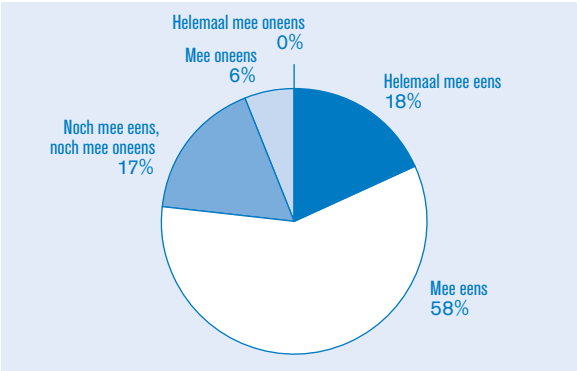
Aan organisaties is de volgende stelling voorgelegd: 'Wij zijn tevreden over de wijze waarop Identity Management momenteel is ingericht.' Uit figuur 5 blijkt dat ruim 30% aangeeft tevreden te zijn over de huidige inzet van Identity Management en dat ruim 30% ontevreden is.

Het meest tevreden zijn organisaties in de sectoren Media, IT & entertainment, Financiële dienstverlening en de Nationale overheid. Het is opmerkelijk dat financiële instellingen zo tevreden zijn, aangezien daar momenteel grootschalige Identity Management-projecten plaatsvinden. Het minst tevreden zijn organisaties in de sectoren Onderwijs, Gezondheidszorg en Detailhandel.

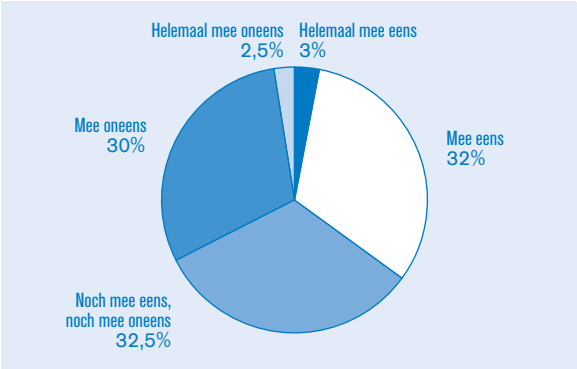
Redenen voor verbetering

Vanwaar de vele Identity Management-projecten? In figuur 6 is te zien wat de meest genoemde redenen voor aanpassing zijn.

Uit de gedetailleerde onderzoeksresultaten blijkt verder dat het reduceren van het aantal authenticatiemiddelen en het integreren van fysieke en logische toegangsbeveiliging, bijvoorbeeld door het multifunctioneel maken van de toegangspas (bijv. smartcard), andere drivers van belang zijn.



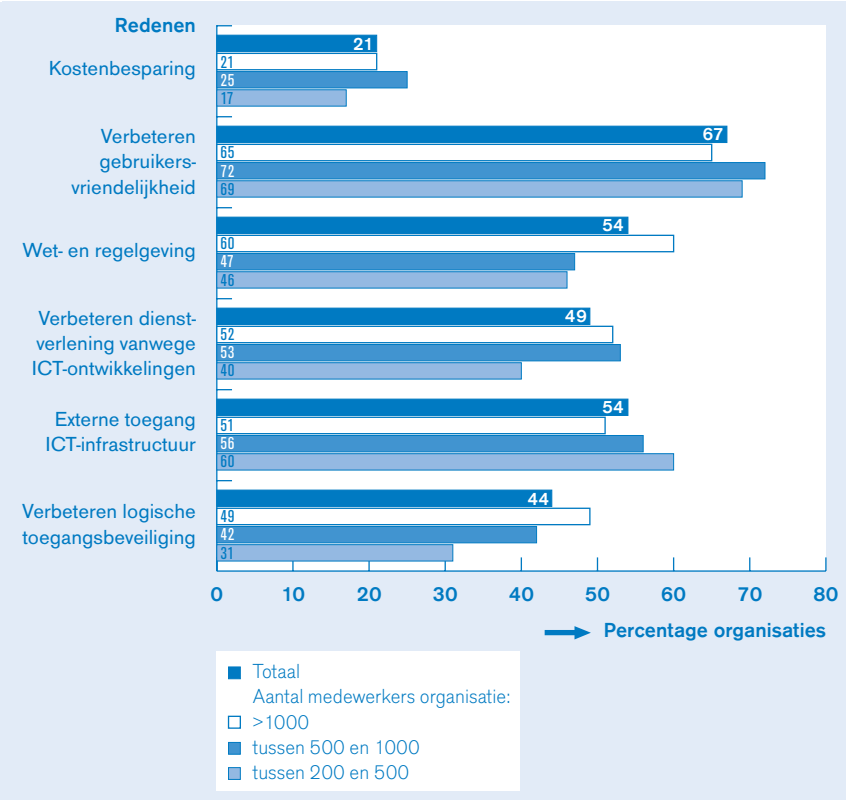
Figuur 4. Reacties op de stelling: Identity Management is enabling technology.

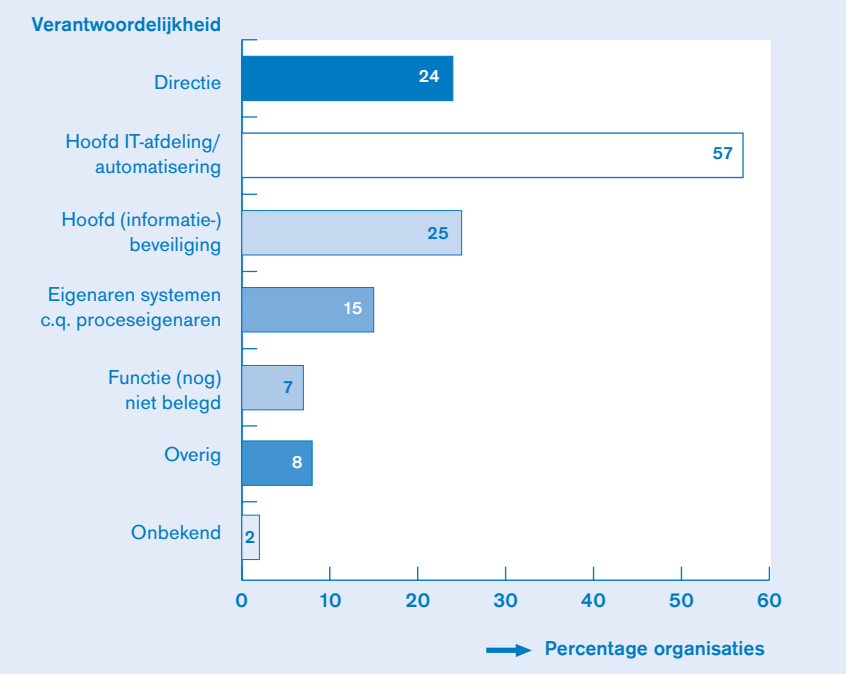


Figuur 5. Reacties op de stelling: Wij zijn tevreden over de wijze waarop Identity Management momenteel is ingericht.

In tegenstelling tot de verhalen van consultants en leveranciers zijn Identity Management-projecten derhalve niet geïnitieerd als kostenbesparingsoperatie, maar voornamelijk voor het verbeteren van de gebruikersvriendelijkheid en het 'in control' zijn c.q. naleving van externe en interne richtlijnen.

Figuur 6. Redenen voor aanpassen van Identity Management.





Figuur 7. Verantwoordelijkheid voor Identity Management.

Verantwoordelijkheid

In figuur 7 is te zien dat bij de helft van de organisaties de verantwoordelijkheid voor Identity Management is belegd in de gebruikersorganisatie (directie, informatiebeveiliging, proces/systeemeigenaren) en bij de andere helft in de ICT-organisatie (hoofd ICT-afdeling). Gezien het door ons in de praktijk waargenomen technische karakter waarmee diverse organisaties dit onderwerp benaderen, verbaast het ons niet dat deze verantwoordelijkheid nog niet bij alle organisaties aan de gebruikerszijde is geplaatst.

Het is ook gebleken dat het niet toekennen van verantwoordelijkheden gerelateerd is aan het niet beschikken over beleid op Identity Management-gebied.

Authenticatiemiddelen

De door onderzoeksbureaus voorspelde sterke opkomst van alternatieven voor wachtwoorden blijkt maar beperkt bewaarheid te worden. Het gebruik van tokens en digitale certificaten neemt geleidelijk toe, waarbij softwarecertificaten uit kostenoverwegingen veelal de voorkeur krijgen (zie figuur 8). Het succes van biometrische beveiliging lijkt sterk afhankelijk te zijn van grootschalige introductie door de overheid (nationale identiteitskaart, zorgpas, e.d.).

Delen van authenticatiemiddelen

Uit figuur 9 blijkt dat in 71% van de organisaties sprake is van het incidenteel of structureel delen van authenticatiemiddelen zoals wachtwoorden. Dit betekent dat het handhaven van functiescheidingen en het naleven van bijvoorbeeld de Wet bescherming persoonsgegevens moeilijk of geheel niet is af te dwingen. Tevens zijn mutaties niet meer herleidbaar tot de persoon die ze heeft aangebracht.

Toekennen van autorisaties

De wijze waarop autorisaties worden toegekend aan gebruikers varieert van het kopiëren van bestaande accounts en/of templates (52%) tot aan Role-Based Access Control (RBAC) (37%). Bij slechts 1% van de organisaties hebben geauthenticeerde gebruikers toegang tot alle ICT-objecten. Overigens blijkt in de praktijk dat een individueel autorisatieprofiel afgestemd op iemands functie vaak al wordt gezien als RBAC.

Overzicht en controle van autorisaties

Hoe is het gesteld met de beheermatige aspecten van autorisatiemanagement? In figuur 11 is zichtbaar dat slechts 39% van de organisaties zegt te kunnen beschik-

ken over een juist, volledig en actueel overzicht van verleende autorisaties, 35% geeft aan hierover zeker niet te kunnen beschikken.

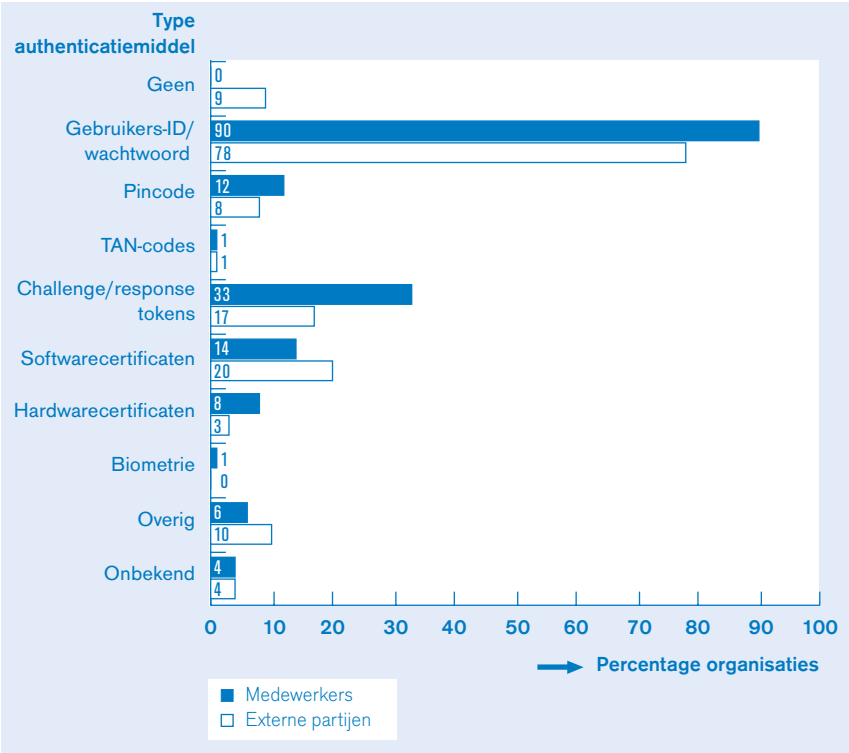
Identity Management functioneert in een dynamische omgeving met betrekking tot gebruikers (bijvoorbeeld verloop van personeel, verandering van taken en rollen van medewerkers, diversiteit in externe medewerkers en klanten) en met betrekking tot de technische systemen en applicaties (nieuwe applicaties, nieuwe applicatieversies, nieuwe platformen en besturingssystemen). Hierdoor is het van belang de inzet van Identity Management regelmatig te controleren. Controle kan vaststellen of toegangsrechten mogelijk te ruim zijn ingesteld en in hoeverre accounts van uit dienst getreden personeel nog bestaan. Dergelijke 'ghost accounts' verlagen het beveiligingsniveau en verhogen de kosten, zeker in het geval van kostbare licenties.

Wat gebeurt er vervolgens met dergelijke overzichten? Bijna de helft van de organisaties (46%) voert periodiek controles uit op uitgegeven autorisaties. Bij 34% worden geen periodieke controles uitgevoerd (zie figuur 12). 13% voert nooit controles uit.

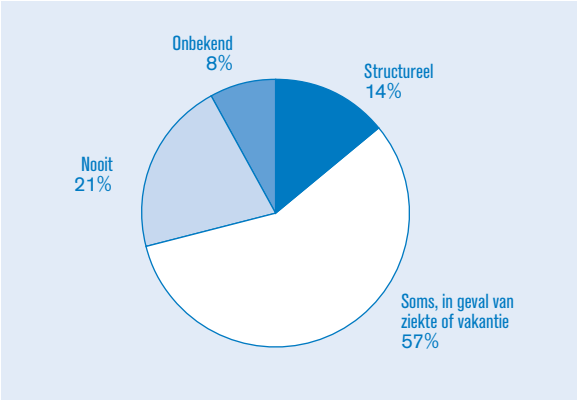
Bovenstaande uitkomsten op het gebied van autorisatiebeheer resulteren in een situatie waarin autorisaties niet geheel of zelfs geheel niet in overeenstemming zijn met de organisatorische eisen en wensen. Een significant deel van de respondenten (36%) geeft namelijk aan dat bij controles vaak blijkt dat autorisaties in hun organisatie te ruim zijn ingesteld en 27% geeft aan dat dit niet het geval is (zie figuur 13).

Onweerlegbaarheid

Onweerlegbaarheid van transacties betekent dat een communicatie of een transactie noch door de zender noch de ontvanger achteraf kan worden ontkend. Organisaties is gevraagd welke maatregelen zijn genomen om

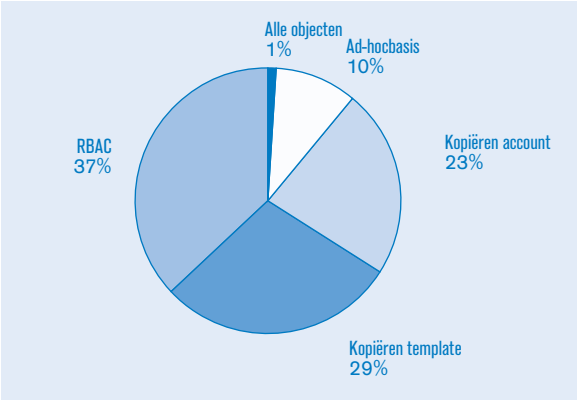


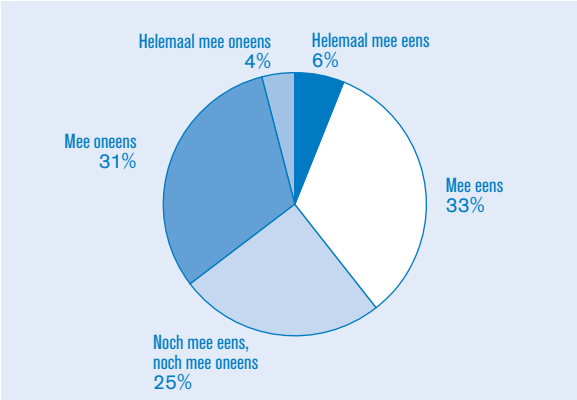
Figuur 8. Type gebruikt authenticatiemiddel.



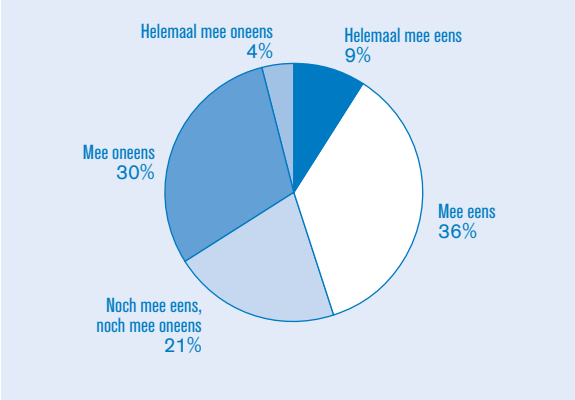
Figuur 9. Delen van authenticatiemiddelen.

Figuur 10. Wijze van autorisatietoekenning.

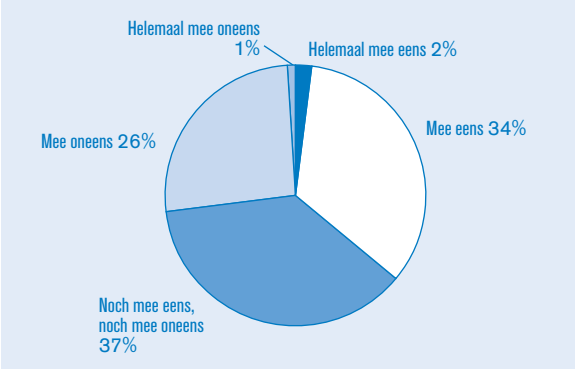




Figuur 11. Reacties op de stelling: Actueel overzicht van verleende autorisaties is beschikbaar.

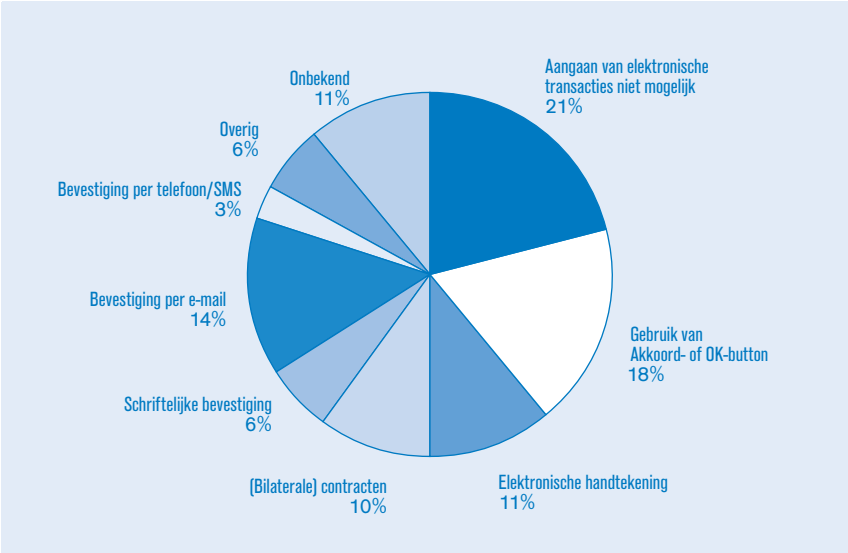


Figuur 12. Reacties op de stelling: Periodiek vindt controle op verleende autorisaties plaats.



Figuur 13. Reacties op de stelling: Autorisaties zijn te ruim ingesteld.

Figuur 14. Maatregelen voor onweerlegbaarheid.



de onweerlegbaarheid van elektronische transacties te kunnen waarborgen. De resultaten staan in figuur 14 weergegeven. Om transacties formeel te kunnen accorderen wordt vooral gebruikgemaakt van eenvoudige oplossingen, zoals een 'OK'-knop (18%) of bevestiging per e-mail (14%), telefoon of SMS (3%). Hierbij moet worden opgemerkt dat deze maatregelen op zich onweerlegbaarheid vanuit juridisch oogpunt niet afdoende kunnen waarborgen.

Sinds de invoering van de wet Elektronische Handtekening medio 2003 is het technisch mogelijk de onweerlegbaarheid van elektronische transacties te garanderen en hier zelfs een juridische consequentie aan te koppelen. Ondanks dat de elektronische handtekening relatief recentelijk wettelijk en technisch mogelijk is geworden, gaf inmiddels al 11% van de respondenten aan gebruik te maken van een vorm van een elektronische handtekening.

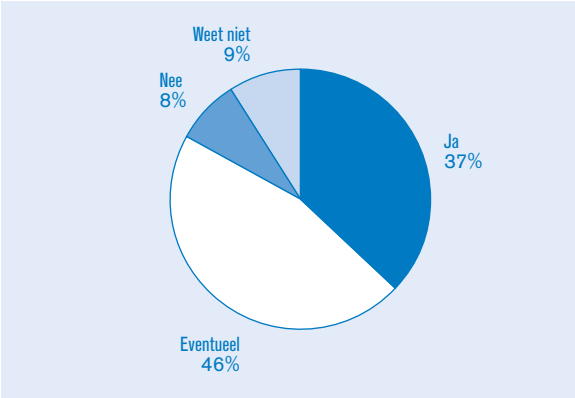
Uitbesteding

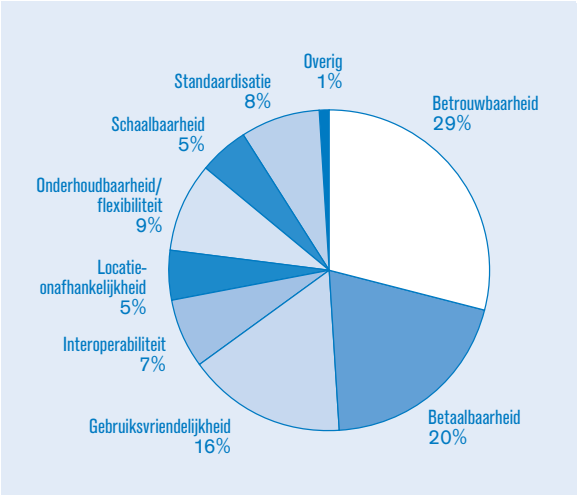
Figuur 15 geeft een verrassend hoge uitkomst inzake mogelijke uitbesteding op authenticatiegebied. 84% van de organisaties zal zeker of eventueel gebruik gaan maken van authenticatiediensten en -middelen die door een andere partij worden verstrekt.

In figuur 16 zijn de belangrijkste redenen om van authenticatiediensten van derden gebruik te maken opgenomen. Dit zijn met name betrouwbaarheid, betaalbaarheid en gebruikersvriendelijkheid.

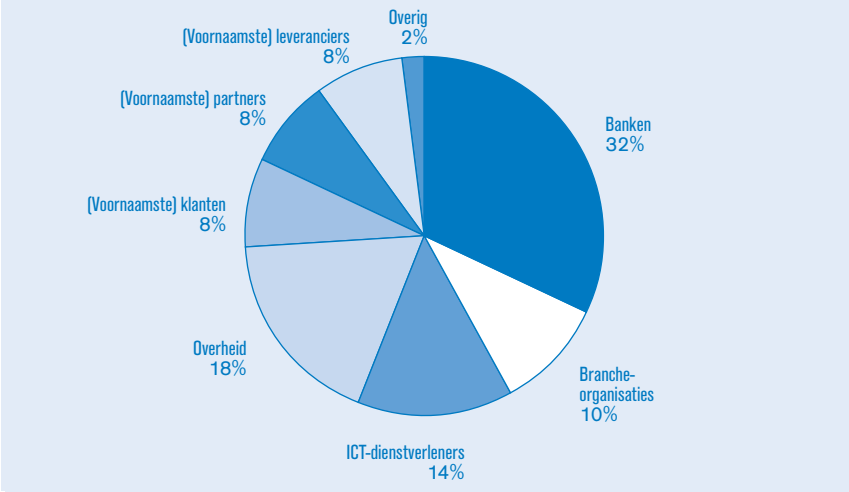
Diverse organisaties blijken in aanmerking te komen om deze authenticatiediensten te leveren, maar banken (32%), overheid (18%) en ICT-dienstverleners worden het meest genoemd (zie figuur 17).

Figuur 15. Uitbesteding van authenticatiediensten.





Figuur 16. Redenen voor uitbesteding van authenticatie.



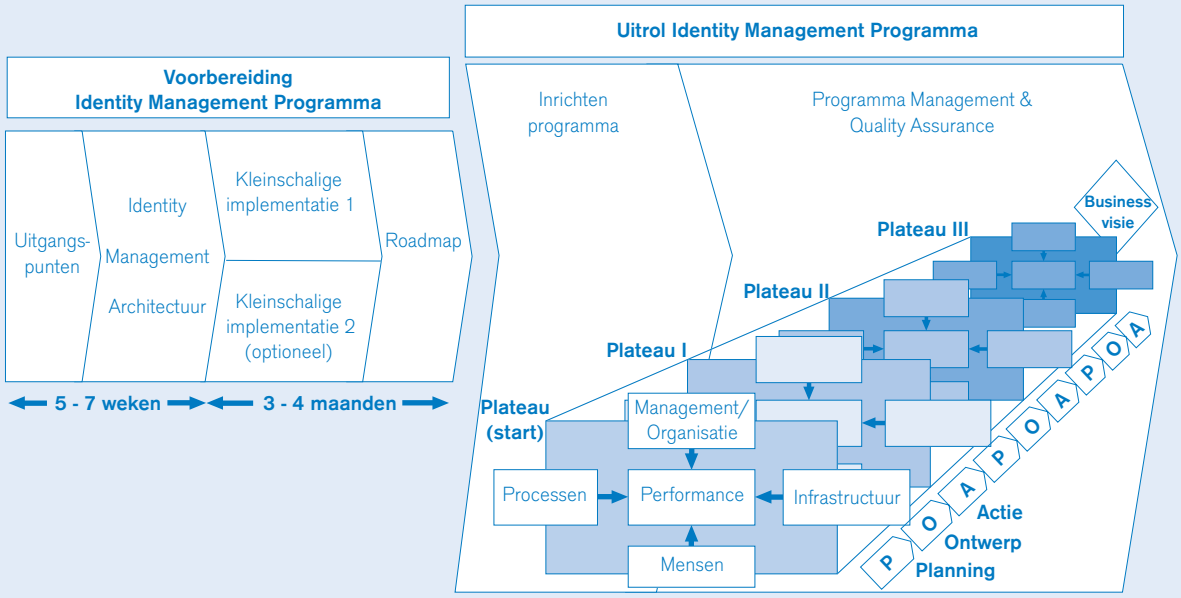
Figuur 17. Uitbestedingspartij voor authenticatiediensten.

De behoefte aan een betere inrichting van Identity Management wordt breed onderkend:
- noodzaak tot betere grip en controle op autorisaties (ingegeven door regelgeving);
- noodzakelijke reductie van de (administratie)kosten van de helpdesk;
- verhoging van de kwaliteit van de ICT-dienstverlening aan de (interne) klant.

Echter, het invoeren van Identity Management is geen sinecure:
- Invoering van Identity Management is complex, het raakt zowel de gehele ICT-omgeving als de organisatie.
- Hoewel de problematiek in generieke zin speelt voor iedere organisatie, is het noodzakelijk te onderkennen dat de invoeringsstrategie per organisatie verschilt.

Binnen de invoeringsstrategieën kunnen diverse invoeringsparameters worden onderkend, zoals:
– doelgroepen van gebruikers;
– platformen;
– applicaties;
– organisatorische eenheden;
– fysieke locaties,

alsmede de prioriteitstelling vanuit de organisatie (bijv. door een ERP- of SOX-project). Op basis van deze parameters zal de invoeringsstrategie voor een organisatie worden bepaald.



Kader 1. KPMG Identity Management-projectaanpak – Pragmatisch vanuit een visie!

• Een succesvolle invoering vereist specialisme in kennis en ervaring, vaak aangevuld met tooling. Door de hoeveelheid gebruikers, authenticatiemiddelen en autorisaties is het ons inziens niet goed mogelijk zonder inzet van geautomatiseerde hulpmiddelen een efficiënt en effectief Identity Management in te voeren.

Om genoemde redenen heeft KPMG Information Risk Management een programma-aanpak ontwikkeld, *KPMG Identity Management in Control* genaamd, welke zich in de praktijk al meermalen heeft bewezen. Deze aanpak kenmerkt zich door pragmatiek met en vanuit een visie, gericht op een structureel langetermijnresultaat, gecombineerd met een zichtbaar kortetermijnrendement.

Op hoofdlijnen bevat de Identity Management-aanpak de volgende stappen:
• Na een korte inventarisatie van de uitgangspunten of een vaststelling van de visie en het opstellen van de Identity Management-blauwdruk, is de aanpak gericht op het op korte termijn realiseren van een aantal 'quick wins'. Dit kan worden bereikt met het uitvoeren van een aantal kleinschalige implementaties ter toetsing van de toepasbaarheid van het Identity Management-concept in één of meer organisatieonderdelen. De kleinschalige implementaties zijn gericht op het inrichten en verbeteren van de verschillende Identity Management-functionaliteiten, zoals daar zijn gebruikers-, authenticatie- en autorisatiemanagement, alsmede het verbeteren van de controleerbaarheid met auditing- en loggingfuncties.
• Na deze kleinschalige implementaties wordt een stappenplan ('Identity Management Roadmap') opgesteld voor de te doorlopen vervolgactiviteiten op de verschillende Identity Management-gebieden. De stappen leiden tot beheersbare plateaus met een stabiele functionaliteit van waaruit de vervolgstap is te maken – wederom op basis van de evaluatie van de gerealiseerde situatie en de kosten-batenverhouding van vervolgstappen. Dit voorkomt het ontstaan van één langdurig, kostbaar en moeilijk beheersbaar project met constante wijziging van alle elementen.
• Onder coördinatie van een op te zetten Identity Management-programma(bureau) zullen vervolgens separate projecten het uiteindelijke resultaat moeten realiseren: 'Identity Management in control'.

Conclusie

We concluderen uit de onderzoeksresultaten dat Nederlandse organisaties niet 'in control' zijn. De problemen met het wijdverbreid delen van authenticatiemiddelen en matig gemanagede autorisaties zorgen ervoor dat er grote risico's bestaan in de vorm van beveiligings- en privacyincidenten, fraude, identiteitsdiefstal en dergelijke. Een soortgelijk beeld komt naar voren uit ICT-audits die wij als KPMG uitvoeren. De uitkomsten wijzen er ook op dat relevante wet- en regelgeving bij diverse organisaties niet wordt nageleefd!

Overigens blijkt uit het onderzoek wel dat organisaties hun processen voor het toekennen van authenticatiemiddelen en autorisaties hebben verbeterd en grotendeels geüniformeerd. Wel is er veelal een oplossing per applicatie, ICT-omgeving of organisatieonderdeel in gebruik. Dit gaat nog niet altijd gepaard met meer structurele verbeteringsactiviteiten, zoals:
• het standaardiseren van authenticatiemanagement;
• het toepassen van autorisatierollen;
• het inbedden in de beveiligingsarchitectuur en ICT-infrastructuur;
• het centraliseren van de Identity Management-functie;
• het verbeteren van de efficiëntie met specifieke Identity Management-software.

Voor het realiseren van een dergelijk volwassenheidsniveau op Identity Management-gebied is een gedegen aanpak onontbeerlijk. Met de in dit artikel geschetste aanpak en stappen valt – zo is in de praktijk gebleken – een structurele verbetering te bewerkstelligen.

Literatuur

[KPMG03] *Executive Summary Identity Management Survey 2003*, KPMG, november 2003 (per e-mail op te vragen bij de auteurs).
[KPMG02] *Global Information Security Survey 2002*, KPMG, maart 2002.
[Mien03] Ing. P. Mienes RE en B. Bokhorst RE RA, *De (on)beheersbaarheid van toegangsbeveiliging*, Compact 2003/1.